Strategic and Analytics-Driven Inspection Operations for Critical Infrastructure Resilience

by

Mathieu Dahan

B.S., Paris-Sud University (2013)
M.S., École Centrale Paris (2016)
S.M., Massachusetts Institute of Technology (2016)

Submitted to the Department of Civil and Environmental Engineering
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Civil Engineering and Computation

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2019

Author .....
Department of Civil and Environmental Engineering
May 17, 2019

Certified by .....
Saurabh Amin
Associate Professor of Civil and Environmental Engineering
Thesis Supervisor

Accepted by .....
Heidi Nepf
Donald and Martha Harleman Professor of Civil and Environmental Engineering
Chair, Graduate Program Committee

Accepted by .....
Nicolas Hadjiconstantinou
Professor of Mechanical Engineering
Co-Director, Center for Computational Engineering

Strategic and Analytics-Driven Inspection Operations for Critical Infrastructure Resilience

by

Mathieu Dahan

Submitted to the Department of Civil and Environmental Engineering
on May 17, 2019, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Civil Engineering and Computation

Abstract

Resilience of infrastructure networks is a key requirement for a functioning modern society. These networks work continuously to enable the delivery of critical services such as water, natural gas, and transportation. However, recent natural disasters and cyber-physical security attacks have demonstrated that the lack of effective failure detection and identification capabilities is one of the main contributors of economic losses and safety risks faced by service utilities. This thesis focuses on both strategic and operational aspects of inspection processes for large-scale infrastructure networks, with the goal of improving their resilience to reliability and security failures. We address three combinatorial problems: (i) Strategic inspection for detecting adversarial failures; (ii) Strategic interdiction of malicious network flows; (iii) Analytics-driven inspection for localizing post-disaster failures. We exploit the structural properties of these problems to develop new and practically relevant solutions for inspection of large-scale networks, along with approximation guarantees.

Firstly, we address the question of determining a randomized inspection strategy with minimum number of detectors that ensures a target detection performance against multiple adversarial failures in the network. This question can be formulated as a mathematical program with constraints involving the Nash equilibria of a large strategic game. We solve this inspection problem with a novel approach that relies on the submodularity of the detection model and solutions of minimum set cover and maximum set packing problems.

Secondly, we consider a generic network security game between a routing entity that sends its flow through the network, and an interdictor who simultaneously interdicts multiple edges. By proving the existence of a probability distribution on a partially ordered set that satisfies a set of constraints, we show that the equilibrium properties of the game can be described using primal and dual solutions of a minimum-cost circulation problem. Our analysis provides a new characterization of the critical network components in strategic flow interdiction problems.

Finally, we develop an analytics-driven approach for localizing failures under uncertainty. We utilize the information provided by failure prediction models to calibrate

the generic formulation of a team orienteering problem with stochastic rewards and service times. We derive a compact mixed-integer programming formulation of the problem that computes an optimal a-priori routing of the inspection teams. Using the data collected by a major gas utility after an earthquake, we demonstrate the value of predictive analytics for improving their response operations.

Thesis Supervisor: Saurabh Amin
Title: Associate Professor of Civil and Environmental Engineering

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my advisor Saurabh Amin, without whom this thesis would certainly not exist. I am very grateful for everything he has done for me, for the tremendous amount of time he devoted to this work, and for his unconditional guidance and support during the past five years. It has been a great honor and pleasure to work with him.

I would also like to thank Patrick Jaillet, Georgia Perakis, and Ali Jadbabaie for serving on my thesis committee. They have provided me with insightful comments and suggestions that significantly helped in shaping the work in this thesis. I have also been very fortunate to collaborate with Patrick and Georgia, from whom I learned a lot. I sincerely appreciate their time and guidance towards the completion of this thesis. I am also very grateful to Jim Orlin for giving me the opportunity to TA for him. It was a real pleasure interacting with these amazing researchers and teachers during my time at MIT.

I would like to thank my other coauthors for the great projects they enabled me to be part of. I owe a special thanks to Lina Sela and Andrew Lee. Working with them significantly helped me deepen my understanding and increase my knowledge on the topics involved in this thesis. I would also like to thank my lab mates, who continuously provided insightful comments and helped improve my research projects.

My time at MIT would not have been the same without all the great people that I met there, especially from the Operations Research Center. I really enjoyed all the good times we have had altogether. I am especially grateful to have had Diana in my life for the past two years. Her support and care significantly helped me go through the obstacles faced at the end of my PhD.

Finally, I am deeply grateful to my family for their undying support throughout all these years. I especially cannot thank my parents enough for everything they have done for me. I owe them everything.

The work in this thesis was supported in part by the Singapore National Research Foundation through the Singapore MIT Alliance for Research and Technol-

ogy (SMART), the DoD Science of Security Research Lablet (SOS), MIT Schoettler Fellowship, FORCES (Foundations Of Resilient CybEr-Physical Systems), which receives support from the National Science Foundation (NSF award numbers CNS-1238959, CNS-1238962, CNS-1239054, CNS-1239166), NSF CAREER award CNS-1453126, and the AFRL LABLET - Science of Secure and Resilient Cyber-Physical Systems (Contract ID: FA8750-14-2-0180, SUB 2784-018400).

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation: Infrastructure Resilience

Critical infrastructure networks, such as electricity, water, and transportation networks, are essential for our modern society. These systems work continuously to enable the delivery of essential services from diverse resources to diverse loads through physical networks that are comprised of heterogeneous, interconnected components. These infrastructure components are numerous and diverse in type, behavior, and vulnerabilities, and need to be monitored to ensure their operation. Indeed, these components are routinely subject to reliability failures due to aging infrastructure, as well as security threats from malicious entities. Therefore, ensuring the resilience of these infrastructure networks against reliability and security failures is crucial for ensuring the availability and quality of the essential services that rely on these networks.

Many utilities and their customers face significant issues related to the service quality and reliability of supply, as evident by recurrent (and often disastrous) incidents [64, 70]. These incidents are becoming more frequent due to the deteriorating state of infrastructure and the high-intensity natural events that many parts of the world are facing [52]. For instance, electricity and transportation networks are directly impacted by the increase in the number of hurricanes that the past thirty years have witnessed.

In addition, recent incidents have demonstrated that malicious entities can disrupt or gain control of these systems by exploiting cyber vulnerabilities or physical faults, or their combination. Indeed, sophisticated cyber intrusions, e.g., BlackEnergy3 [65], Stuxnet [32], physical attacks, e.g., Metcalf power substation sniper attack [98], and the significant increase in the number of successful incidents over the past ten years [9, 20, 25, 31, 40, 51, 63, 75, 79, 86, 96], confirm the insufficiency of the existing protection solutions. Such incidents can cause correlated failures, resulting in significant economic losses, and even loss of human lives.

Since resiliency was not considered at the design stage of existing infrastructure systems, there is a need to improve the utilities' situation awareness to security attacks, as well as its operational readiness to respond to failures caused by natural disasters. The goal of this thesis is to develop a foundational approach for strategic security planning and operational response design, so that our infrastructure systems can better withstand, recover from, and adapt to both random and adversarial failures. For strategic planning, we focus on designing inspection strategies to monitor large-scale infrastructure systems that face risks of random failures and security attacks. For operational response in the aftermath of a natural disaster, we study the problem of scheduling inspection operations assisted by predictive analytics to localize component failures. In particular, we exploit the features of the problems to develop scalable and implementable solution approaches, along with optimality guarantees. Through this thesis, we contribute to methods in network and combinatorial optimization, computational game theory, and predictive analytics.

1.2 Thesis Focus: Inspection Operations

Inspection systems for monitoring critical infrastructure networks play a crucial role in providing situational awareness to the distribution utilities, who are tasked with maintaining the functional state and service quality of their expansive assets. During the last two decades, utilities have started to deploy new sensing, communication, and control technologies to detect a variety of incidents and improve their operations.

1.2.1 Current Operations and Challenges

Consider the inspection problem faced by a utility company (typically a regulated monopoly) that manages a natural gas pipeline network in an urban area. Traditionally, utility personnel conduct inspections of network assets and customer connections at a predetermined frequency (once every 2-4 years), or when an emergency situation is reported [72]. The main challenges faced by these inspection systems are threefold:

1) Utility companies do not have enough resources to continuously monitor every component. Thus, current inspection operations tend to prioritize major components such as main lines and valve stations. As a result, the detection of minor leaks is delayed, often causing significant damages in the future: for instance, minor gas leaks occasionally evolve to become major explosions.

2) In many situations, utility crews do not have an immediate access to the diagnostic information about the type or location of failure events. Consequently, the actual response times often exceed the time to failure, resulting in major losses to utilities and safety risks to both customers and utility personnel. In addition, this increase in response time also impacts the cost of utilities' inspection operations, as they may dispatch their inspection teams to locations that do not contain failures.

3) Physical or remote access to critical components can be exploited by malicious entities. These entities may use a combination of physical and digital tampering to bypass safety systems. However, inspection systems typically do not account for strategic and resourceful attackers whose actions are more difficult to detect, in comparison to isolated random failures.

In summary, although current inspection systems are configured to provide situational awareness to the system operator under nominal conditions, they only provide limited and uncertain information when a major event occurs (e.g., natural disaster or security attack). Since utilities are operating a large number of components with

limited resources, these challenges result in inspection systems with limited performances, which in turn result in infrastructure networks being less resilient to reliability and security failures.

1.2.2 New Opportunities

Fortunately, recent advances in sensing technologies have resulted in commercially available smart detector systems, which include a sensor, a detection software, and a communication unit [22, 108]. These detectors can be easily operated by the utility personnel and flexibly positioned in the network for timely detection of failure events. For example, wireless sensor networks have been successfully used in the monitoring of water networks [5, 100]. These sensors provide timely and accurate data to enable the detection of possible pipeline breaks and contamination events [89]. Sensor networks are also being utilized to monitor oil and natural gas networks [110]. By adopting smart detectors in their inspection operations, the utilities can at least partly address the aforementioned limitations [90].

In addition, Unmanned Aircraft Systems are rapidly emerging as a deployable imagery asset, which can be tasked in a manner similar to the fixed vision sensors, but with mobility as a constraint. Significant advancements in autonomous systems during the past 15 years have resulted in rapidly deployable, low-cost small Unmanned Aircraft Systems (sUAS) with heterogeneous sensing modalities, for example, onboard electro-optical and infrared sensors. Typical use cases include executing reconnaissance and surveillance operations for command and control centers. More recently, widespread commercial availability of sUAS has generated significant interest in using them for situational awareness in urban environments. The opportunity to use sUAS as monitoring systems is especially promising in a range of infrastructure applications such as detection of power line failures, clearance of highway incidents, and identification of pipeline bursts.

Finally, these new technologies also enable service utilities to acquire data regarding their inspection operations. In addition to publicly available information, such operational data can significantly improve the diagnostic information regarding the

type and location of failures within their infrastructure network. For example, the increase in the number of crowdsourcing apps where users can report incidents proves to be of interest for assessing the damage of the utilities' extensive assets.

1.2.3 Research Statement

The goal of this thesis is then to develop tools based on predictive analytics, combinatorial optimization, and game theory, to improve the service operations of large-scale critical infrastructures. First, we exploit the newly acquired data (from their previous inspection operations and public sources) to improve the prediction of failure locations. We then integrate the diagnostic information into decision models that focus on scheduling inspection and response operations. Specifically, we consider a network and strategic modeling approach that captures the important features of the problem and improves the strategies of the utilities. We illustrate this overall approach in Figure 1-1.

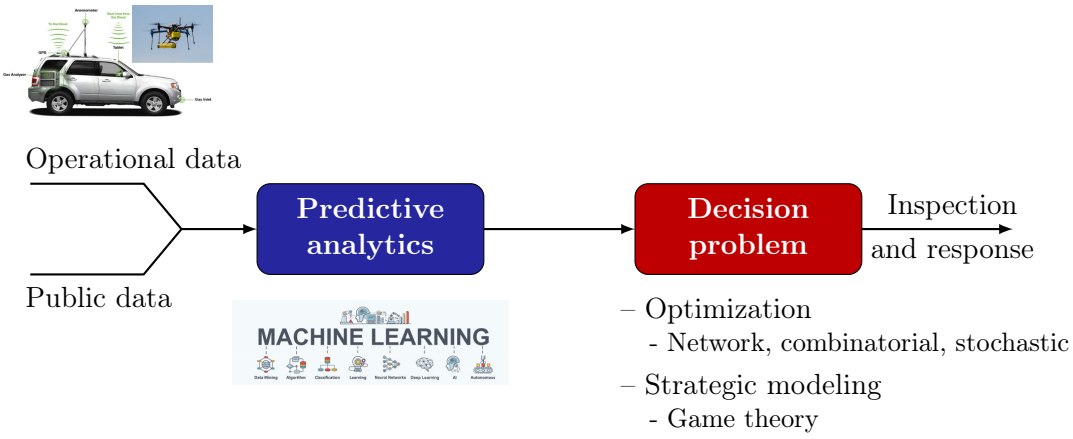


Figure 1-1: Our focus.

In this thesis, we develop this approach to improve inspection operations both before and after a failure event occurs. For pre-event operations, we study how to optimally allocate both fixed and mobile detectors to monitor infrastructure networks against faults and attacks. The goal is to allocate detectors so that when a failure event occurs within the network, it is detected in a timely manner. This is crucial

for facilitating the response operations. Then, after a failure event occurs, we propose an analytics-based approach that improves the diagnostic information, and then integrates it into the problem of dispatching inspection teams for localizing failures. Improving both pre- and post-event inspection operations is crucial for cyber-physical security and disaster response problems, and for improving the resilience of infrastructure networks; see Figure 1-2.

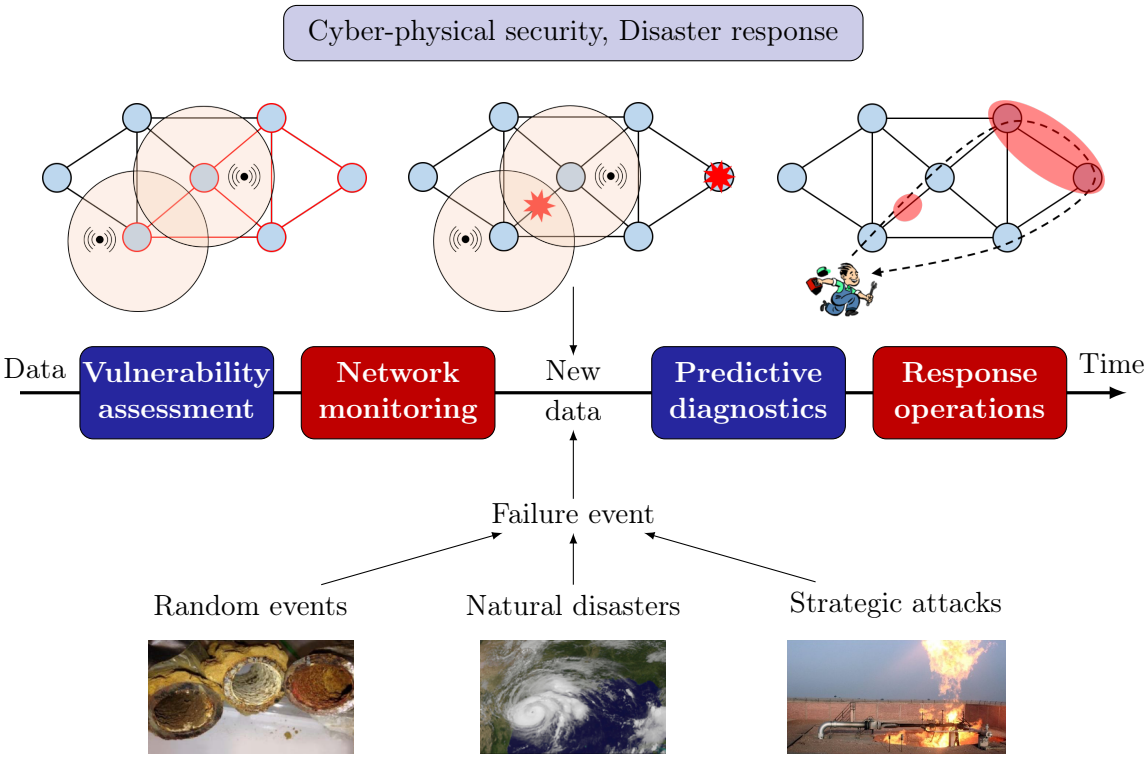


Figure 1-2: Inspection operations for critical infrastructure resilience.

More specifically, this thesis addresses the following three questions (summarized in Figure 1-3):

1. How many detectors are required and how to strategically position them in the network to detect multiple adversarial attacks?

2. How to strategically coordinate multiple interdictors to prevent the routing of illegal goods in a flow network?

3. How to optimize the scheduling of monitoring resources for post-disaster inspection under diagnostic uncertainty?

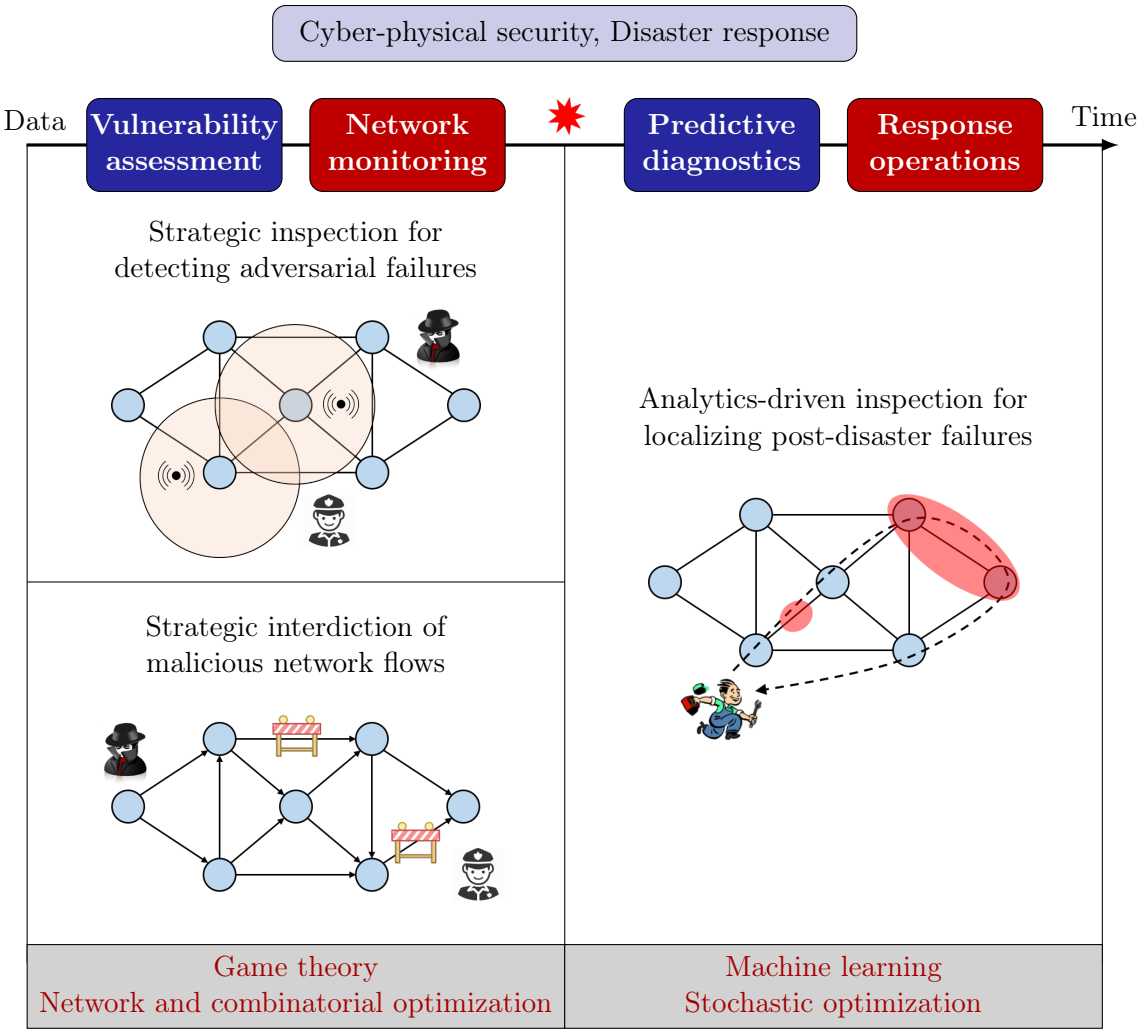


Figure 1-3: Thesis overview.

1.3 Thesis Contributions

Strategic Positioning of Detectors. In this work, we investigate how the currently available smart detector systems – with on-board sensors and data processing/transmission capabilities – should be positioned in a large-scale network to obtain detection guarantees against multiple failure events. This problem is relevant to applications such as sensing of methane leaks, pipeline bursts, and water contamination events. In these applications, the performance of inspection strategies should be evaluated against worst-case events. We approach this problem by considering a

game-theoretic model of interaction between the utility operator who can position a fixed number of detectors, and an adversary who can target one or more network components. The operator's payoff is given by a submodular detection function which counts the components whose failure can be successfully detected. Similarly, the adversary's payoff is the number of components whose failure cannot be detected. The action set of each player is determined by the limited number of available resources. Despite its modeling simplicity, the extremely large size of this game precludes the applicability of known algorithms [69].

To design a good inspection strategy and evaluate its performance, we develop a new scalable approach to study the expected fraction of detected failures – which we refer to as detection rate – in any mixed strategy Nash equilibrium of the above-mentioned game. Firstly, we prove that by inspecting a subset of nodes in a randomized manner and ensuring that each component is monitored with a non-zero probability, the operator can obtain a strictly better detection performance than any fixed positioning of detectors. Secondly, we provide lower and upper bounds on the detection rate in terms of the optimal values of minimum set cover (MSC) and maximum set packing (MSP) problems, as well as the operator's available resources. Thirdly, we construct an approximate equilibrium strategy profile based on solutions of the MSC and MSP problems. In particular, we show that the detection performance for an MSC-based inspection strategy is close to the actual equilibrium detection rate in practical settings. Finally, we show a rather surprising property that the equilibrium detection rate in large networks can be evaluated by considering that the adversary only has a unit attack resource. This implies that an MSC-based inspection strategy can be further refined using a column generation algorithm.

Our proofs are based on game-theoretic arguments and combinatorial properties of the network inspection problem. In particular, we employ linear programming duality in zero-sum games, properties of the MSC and MSP problems, and submodularity of the detection function. The richness and generality of our solution approach make it applicable to various network inspection settings [92], and even extend results of a large class of game-theoretic models [57, 71]. The detection function used in our

formulation can also be refined to capture features such as probability of detection and criticality of components. Most importantly, our approach can be used to design practical inspection strategies that use minimum number of detectors and achieve the target detection performance against worst-case or adversarial failure events.

Strategic Interdiction in Flow Networks. In this work, we study the usefulness of game theory for designing network inspection strategies against a malicious entity (router). In particular, we consider an interdiction process by an agency who seeks to intercept a flow of illegal goods (smuggled drugs, weapons, etc.) through a supply-demand network. In this setting, the agency needs to anticipate how the strategy of the malicious router might change in the presence of interdiction points. Prior work in this area [115] considers bilevel optimization formulations and solves them using mixed integer programming techniques. These models assume that the agency chooses its interdiction plan to induce a maximum lost flow for the router, who chooses her initial flow after observing the agency's plan. This assumption leads to fixed interdiction plans that are not optimal for inspecting strategically chosen route flows.

By contrast, our work shows that by modeling the interaction between the agency and router as a strategic game, we can account for a richer class of malicious router's strategies, and design randomized interdiction plans to impose an optimal strategic flow interdiction. In our model, the router sends her flow through the network while facing heterogeneous path transportation costs; and the agency simultaneously chooses an interdiction plan comprised of one or more edges. The router (resp. agency) seeks to maximize the value of effective (resp. interdicted) flow net the transportation (resp. interdiction) cost. We obtain a characterization of the routes that are likely to receive malicious flows, and the edges that need to be interdicted with non-zero probability.

Importantly, a departure of our analysis from the existing literature is the finding that classical interdiction plans based on minimum capacity cutsets do not fully exploit the agency's interdiction capability. Instead, we discover that an optimal interdiction plan satisfies a set of constraints which ensure that the corresponding

marginal edge interdiction probabilities are equal to the dual solutions of a minimum cost circulation problem. Moreover, an equilibrium strategy of the malicious router maximizes the route flows that cross edges with high interdiction costs, and such a strategy is given by the primal solution of our circulation problem. This imposes another set of constraints on the minimum probability with which each route needs to be interdicted. Since an interdiction plan in our model is a randomized strategy over subsets of edges, it is natural to inquire about the existence of a strategy that satisfies the two sets of equilibrium constraints.

To address this question, we prove a more general result on the existence of a probability distribution on a finite poset that satisfies a set of constraints involving marginal probabilities of the poset's elements and maximal chains. Resolving this existence problem is equivalent to solving a linear optimization program with exponentially many variables and constraints. We positively answer this question by designing a combinatorial algorithm which solves the linear program. Each iteration of the algorithm involves selecting subsets of poset elements and assigning weights to them in a manner that all the equilibrium constraints are satisfied when the algorithm terminates. This result demystifies the complexity of equilibrium computation for our game-theoretic model. Computing an equilibrium interdiction plan is NP-hard due to the enumeration of maximal chains in our algorithm. However, the marginal edge interdiction probabilities and route flows can be obtained in polynomial time by solving the minimum cost circulation problem.

Analytics-Driven Response Operations. This work deals with the problem of optimal scheduling of response operations under imperfect diagnostic information regarding failure locations. We model this problem as a stochastic orienteering problem, which consists of finding a scheduling of sites to inspect that maximizes the expected reward obtained from successfully addressing failures in the network. To overcome the challenge in computing an optimal strategy for large-size networks, we identify key features of optimal solutions to develop a compact mixed-integer programming-based solution approach. Our approach leads to practical strategies which prescribe an a priori response schedule. Importantly, it captures the essential tradeoff between

the travel time between sites and the inspection time of each site, given the imperfect diagnostic information, distances between sites, and available response time. These results demonstrate the advantages of integrating predictive models of failures into emergency response operations.

The rest of this thesis is organized as follows: In Chapter 2, we study the strategic inspection problem for detecting adversarial failures. In Chapter 3, we study the strategic interdiction of malicious network flows. In Chapter 4, we study the analytics-driven inspection problem for localizing post-disaster failures. In Chapter 5, we present an overall summary of the thesis contributions, and discuss future research directions for improving infrastructure resilience.

Chapter 2

Strategic Inspection for Detecting Adversarial Failures

2.1 Introduction

In this chapter, we study a network inspection problem in the face of simultaneous failures cased by a strategic adversary. Our setup is motivated by the need to enhance the capabilities of traditional inspection systems through the use of smart detectors, and achieve a target level of detection performance against incidents, including strategic attacks. Specifically, we consider a game-theoretic formulation of the strategic network inspection problem, and address the question: *How many detectors are required and how to strategically position them in the network to detect multiple adversarial attacks?* Solving this game is challenging because the sets of actions of both players grow combinatorially with the size of the network. Hence, commonly known algorithms [81, 93] cannot be used to compute equilibrium player strategies in a scalable manner. Instead, we construct an approximate equilibrium strategy of this large-scale game based on the properties of minimum set cover and maximum set packing problems. This construction enables a scalable solution approach for our network inspection problem.

2.1.1 Our Contributions

In Section 2.2, we introduce a generic detection model, which captures the key features of modern inspection systems with respect to sensing technology for event detection and flexibility of positioning. Mathematically, the model is represented by a monotone submodular detection function. We use this detection model to define a game-theoretic model of strategic interaction between a defender (inspection agency) and an attacker. The defender chooses where to position her detectors, and the attacker chooses to target one or more network components. Each player is resource-constrained. The defender's objective is to maximize the number of detected attacks, whereas the attacker's objective is to maximize the number of undetected attacks. We adopt mixed strategy Nash equilibrium as the solution concept of this game. We then formulate our inspection problem, denoted $(\mathcal{P})$, as a mathematical program with equilibrium constraints. In this problem, the defender seeks to minimize the number of detectors such that the expected detection rate of attacks (i.e., detection performance) in *any* Nash equilibrium is above a pre-specified threshold.

Essentially, solving the problem $(\mathcal{P})$ involves computing the equilibria of the defender-attacker game. However, the sets of players' actions grow combinatorially with the size of the network, which makes the equilibrium computation challenging. For large-scale networks, the number of available pure strategies for each player n can easily reach 10^{60}. Well-known algorithms such as Lipton et al. [69]'s $n^{O(\ln n/\epsilon^2)}$ time algorithm for computing an $\epsilon-$Nash equilibrium are practically inapplicable for this setting. Instead, in this chapter, we develop a new solution approach based on the properties of minimum set cover (MSC) and maximum set packing (MSP) problems. This approach enables us to solve the problem $(\mathcal{P})$ in a scalable manner and also provide performance guarantees.

Our equilibrium analysis in Section 2.3 consists of first studying useful structural properties that are satisfied by all Nash equilibria of the defender-attacker game. We present these properties for the most conservative case when the attacker has the ability to spread her attacks across the network. In particular, we show that

in any equilibrium, both players must randomize their actions and use all available resources, and every network component must be monitored with positive probability (Propositions 2-3). Importantly, while these are game-theoretic results, their proofs also rely on the properties of the detection function, as well as MSCs and MSPs which respectively capture the "coverage" and "spread" of the network.

These properties enable us to derive lower and upper bounds on the expected detection rate in equilibrium in terms of both players' available resources, and the optimal values of the MSC and MSP problems (Theorem 1). Moreover, using solutions of MSC and MSP problems, we construct a strategy profile that not only is an $\epsilon-$Nash equilibrium, but also provides each player a payoff that is $\epsilon-$close to the payoff they would get in any Nash equilibrium (Theorem 2). In Section 2.3.3, we specialize our results to the case when the duality gap between our two combinatorial optimization problems is zero, i.e., when the sizes of the MSCs and MSPs are the same. We show that, for this case, MSCs and MSPs can be directly used to construct a Nash equilibrium of the game (Proposition 4). We also deduce analytical expressions of the players' payoffs and the expected detection rate of failures in any equilibrium (Corollary 1).

These results enable us to derive (in Section 2.4) an exact solution to the network inspection problem for the case when the MSCs and MSPs are of same size, i.e., we provide an analytical expression of the optimum number of detectors, and an equilibrium strategy profile. For the general case (i.e., when the size of MSCs is larger than or equal to the size of MSPs), Theorems 1 and 2 are used to derive an approximate solution to the problem $(\mathcal{P})$, with guarantees on the detection performance and the corresponding optimality gap (Proposition 6).

Although our approach to solve problem $(\mathcal{P})$ relies on the MSC and MSP problems which are known to be NP-hard, we find that modern integer programming solvers can solve large instances of these problems. In particular, in Section 2.5, we show that our solution approach is scalable to large-sized benchmark distribution networks, and can be used to provide good performance guarantees for monitoring against pipeline disruptions and contaminant injection attacks. In addition, we show that our solution

approach is also valid when only approximate solutions of the MSC and MSP problems (obtained from standard greedy or heuristic algorithms) are available instead of the exact ones.

In Section 2.6, we describe additional settings that can be modeled with our game. First, we study a security game on flow networks, in which an interdictor aims at preventing the routing of illegal goods by a malicious entity. Despite the exponential number of possible network paths that can be taken by the malicious entity, we extend our solution approach by computing a maximum set of edge-disjoint paths and a minimum cardinality cut-set of the network. The max-flow min-cut theorem guarantees that our proposed strategy profile is a Nash equilibrium of the security game. Then, we study a network inspection game in which the operator routes a fleet of small Unmanned Aircraft Systems to detect failures induced by an attacker. We overcome the exponential number of possible inspection paths by formulating two mixed-integer programs that compute our MSC/MSP-based strategy profile.

Although our approach to solving $(\mathcal{P})$ provides a solution with good approximation guarantees in practice, the defender might still prefer to improve that solution. For that purpose, we prove in Section 2.7 that the expected detection rate and the inspection strategies in equilibrium do not depend on the attacker's number of resources if they are smaller than the size of MSPs (Theorem 3). This important and rather surprising structural property is a consequence of the attacker's ability to spread her attacks in the network, and the submodularity of the detection model. From the defender's perspective, this implies that she does not need to know precisely the amount of attack resources. Another implication is that Nash equilibria can be obtained by solving a linear program with a large number of variables but a small number of constraints. Therefore, column generation can be used to iteratively improve our MSC/MSP-based solution. Each iteration provides stronger performance guarantees until it reaches optimality, where the primal and dual solutions give the players strategies in equilibrium. However, the downside is that it can result in an inspection strategy with a large support, which may not be desirable from an implementation perspective. Therefore, a compromise can be reached by running iterations of the

column generation procedure until a tradeoff between the performance and simplicity of the solution is achieved.

Although our results are shown in the case of interest when the attacker has the ability to spread her attacks across the network, we briefly discuss the other case in Section 2.8. Finally, we conclude this chapter by providing the complete proofs of our results in Section 2.9.

2.1.2 Related Work

Our detection model is inspired by modern sensing technology used in detecting leaks and other failure events in pipeline networks for distribution of natural gas [91], and water [84, 97]. A classical problem in sensing of these infrastructure networks is to optimally place sensors for detecting leaks and pipe bursts in the case of reliability failure events. Typically, it can be modeled as a problem of optimal allocation of limited sensing resources to optimize a performance metric, such as observability of the network [21], uncertainty about failure events [62], or proportion of affected population [15]. Some of these formulations can be solved using mixed-integer programming methods, while others exhibit properties of submodular optimization leading to the application of greedy algorithms with approximation guarantees.

Robust formulations of the sensor placement problem have received interest in the literature; for example, Krause et al. [61] proposed an efficient approximation algorithm to maximize the worst-case detection performance against a set of possible failure scenarios. More recently, Orlin et al. [83] and Tzoumas et al. [103] designed approximation algorithms to find a sensor placement that is robust against a subset of sensors' failures. The main feature of this line of work is *fixed sensing*, i.e., continuous operation of sensors placed at fixed locations in the network. On the other hand, our setting is inspired by inspection operations based on smart detectors that can be flexibly positioned in various parts of the network to detect and report incidents. In such settings, it is well-known that *randomized strategies* can significantly improve the defender's performance against worst-case or adversarial failure events [16, 92, 111].

Our game-theoretic model is more general than the classical Hide-and-Seek game

first introduced by Von Neumann [109], and further discussed in Chapter 3.2 of Karlin and Peres [58]. In this zero-sum game, a robber hides in one of a set of "safe-houses" located at roads intersections, and a police unit simultaneously chooses to travel along one road to find the robber. The roads are restricted to be vertical avenues and horizontal streets. Our solution approach can be applied to solve the generalized hide-and-seek game which involves multiple police units patrolling in a complex street network to find multiple robbers. This is possible because our approach can account for multiple player resources, and more realistic monitoring capabilities of the patrolling units. Our game similarly generalizes the Infiltration Game with a Cable, as defined in Chapter 2.1 of Garnaev [37]. In this problem, an infiltrator wants to cross a (discretized) channel and a guard uses an electric cable to detect the infiltrator.

Finally, related to our setting is the work by Mavronicolas et al. [71], who consider a security game on an information network in which the nodes (servers) are vulnerable to multiple attacks and the defender can install a firewall to protect a subnetwork. The defender's goal is to maximize the number of attack detections by randomizing the placement of her firewall. Simultaneously, the attacker's goal is to minimize the number of attacks detected by the firewall. While the authors made the restricting assumption that each subnetwork contains exactly two servers, our detection model can accommodate attack detections within subnetworks of heterogeneous sizes. In fact, our solution approach can be used to derive a defense strategy based on the installation of multiple firewalls to secure the network against multiple simultaneous attacks.

A comparison of these security games is given in Table 2.1.

2.2 Problem Description

In this section, we introduce a generic formulation of strategic network inspection problem based on a game-theoretic model of defender-attacker interaction on the network. Our formulation is a mathematical program with constraints defined in terms of the Nash equilibria of this game.

Table 2.1: Model comparisons.

	Detection model (monitoring locations, components, monitoring sets)			Resources def./att.	Combinatorial objects used for equilibrium characterization	
Our model	$\mathcal{V}$	$\mathcal{E}$	$\mathcal{C}_i,\ i \in \mathcal{V}$	b_1/b_2	MSC	MSP
[58]	Street roads	Safe-houses	Safe-houses located on road i	$b_1 = 1$ $b_2 = 1$	Minimum line cover	Maximum matching
[38]	Cable location	Channel sections	Sections covered from the cable's location i	$b_1 = 1$ $b_2 = 1$	Minimum interval cover	Maximum independent infiltration set
[71]	Network edge	Network nodes	End nodes of edge i	$b_1 = 1$ $b_2 \geq 1$	Minimum edge cover	Maximum independent set

2.2.1 Defender and Attacker Models

Consider the setting where a defender (inspection agency) is concerned with positioning a set of smart detectors in a given network to monitor a predefined set of components, denoted $\mathcal{E}$. The set of locations (or nodes) where a detector can be positioned is also predefined, and is denoted $\mathcal{V}$. All components in the set $\mathcal{E}$ are "critical" in that they are prone to targeted attacks by an attacker (malicious entity). The attacker can simultaneously attack multiple components and compromise their functionality or quality of service. The defender seeks to inspect the network in order to maximize the number of detected attacks. On the other hand, the attacker wishes to avoid being detected (i.e., maximize the number of undetected attacks), so as to reduce the overall functionality of the network.

For our purpose, each *detector* can be viewed as an integrated system comprised of a sensor, a detection software, a communication unit, and a human operator (utility employee) [22]. When a detector is positioned at node $i \in \mathcal{V}$, the following steps are executed: Firstly, the sensor collects relevant state measurements from node i. These measurements capture the operational state of a subset of components $\mathcal{C}_i \in 2^{\mathcal{E}}$. Secondly, the detection software processes these measurements and generates a diagnostic signal indicating the number of attacks present within the component set $\mathcal{C}_i$. Thirdly, the communication unit transmits the diagnostic signal to the defender. Finally, the human operator coordinates all these steps, and also ensures that the

detector system is positioned in the network as intended by the defender. The cost of data collection, processing, and transmission is negligible in comparison to the cost of procuring the detector (which includes the cost of purchasing the equipment and the cost of employing the operator). For a detector positioned at node $i \in \mathcal{V}$, we refer to the set $\mathcal{C}_i$ as a *monitoring set*, because under the aforementioned assumptions, an attack to any component $e \in \mathcal{E}$ can be detected if and only if $e \in \mathcal{C}_i$. The tuple $\mathcal{G} \coloneqq (\mathcal{V}, \mathcal{E}, \{\mathcal{C}_i,\ i \in \mathcal{V}\})$ represents the *detection model* of the network.

We assume that the defender has access to only a limited number of detectors for network inspection. This limitation results from the economic and operational constraints of the defender. For simplicity, we consider that all detectors are homogeneous in terms of their monitoring and detection capabilities, and cost. Let $b_1 \in \mathbb{N}$ be the number of available detectors that can be simultaneously positioned on distinct nodes in $\mathcal{V}$. We denote a *detector positioning* by a set $S \in 2^{\mathcal{V}}$ of nodes that receive detectors. The set of feasible detector positionings is then defined by $\mathcal{A}_1 \coloneqq \{S \in 2^{\mathcal{V}} \mid |S| \leq b_1\}$. For a given detector positioning $S \in \mathcal{A}_1$, let $\mathcal{C}_S \coloneqq \cup_{i \in S} \mathcal{C}_i$ denote the set of components that are monitored by at least one detector in S.

To count the number of components in any given subset of components of $\mathcal{E}$ that can be monitored using an arbitrary detector positioning, we define a *detection function* $\mathrm{F} : 2^{\mathcal{V}} \times 2^{\mathcal{E}} \longrightarrow \mathbb{N}$. Specifically, for a detector positioning $S \in 2^{\mathcal{V}}$ and a subset of components $T \in 2^{\mathcal{E}}$, the value of $\mathrm{F}(S, T)$ is the number of components of T that are monitored by at least one detector positioned in S, i.e.:

$$\forall (S, T) \in 2^{\mathcal{V}} \times 2^{\mathcal{E}}, \quad \mathrm{F}(S, T) \coloneqq |\mathcal{C}_S \cap T| = \sum_{e \in T} \mathbb{1}_{\{e \in \mathcal{C}_S\}}. \tag{2.1}$$

The detection function has two natural properties:

(i) For any subset of components $T \in 2^{\mathcal{E}}$, $\mathrm{F}(\cdot, T)$ is submodular and monotone:

$$\forall T \in 2^{\mathcal{E}},\ \forall (S, S') \in (2^{\mathcal{V}})^2,\ \begin{cases} \mathrm{F}(S \cup S', T) + \mathrm{F}(S \cap S', T) \leq \mathrm{F}(S, T) + \mathrm{F}(S', T), \\ S \subseteq S' \implies \mathrm{F}(S, T) \leq \mathrm{F}(S', T). \end{cases}$$

That is, adding a detector to a smaller detector positioning increases the number

of monitored components in T by at least as many as when adding that detector to a larger detector positioning.

(ii) For any detector positioning $S \in 2^{\mathcal{V}}$, $\mathrm{F}(S, \cdot)$ is finitely additive (a direct consequence of (2.1)):

$$\forall S \in 2^{\mathcal{V}},\ \forall (T, T') \in (2^{\mathcal{E}})^2 \mid T \cap T' = \emptyset, \quad \mathrm{F}(S, T \cup T') = \mathrm{F}(S, T) + \mathrm{F}(S, T').$$

Similar to the defender, the attacker is also resource-constrained, in that she can attack a subset of components $T \in 2^{\mathcal{E}}$ of the network of size no larger than $b_2 \in \mathbb{N}$; we refer to such a subset as an *attack plan*. This limitation arises from the attacker's constraints in gaining an unauthorized access to network components and compromising their functionality. However, the attacker has the flexibility to spread her attacks throughout the network. The set of all attack plans is given by $\mathcal{A}_2 \coloneqq \{T \in 2^{\mathcal{E}} \mid |T| \leq b_2\}$.

2.2.2 Network Inspection Problem

We model the simplest form of strategic interaction in which both players make individual decisions to maximize their objectives. Particularly, for a detector positioning $S \in \mathcal{A}_1$ and an attack plan $T \in \mathcal{A}_2$, the payoff of the defender (resp. attacker) is $\mathrm{F}(S, T)$ (resp. $|T| - \mathrm{F}(S, T)$). Both players have the flexibility of changing their actions from one subset to another. For the defender, this means that her detectors can be repositioned from one subset of nodes to another. Practically, changes in detector positioning are executed by the utility personnel who use manual or automated means to shift detectors.

In our model, the defender (resp. attacker) inspects (resp. attacks) the network using a detector positioning S (resp. an attack plan T) realized from a chosen probability distribution on the set $\mathcal{A}_1$ (resp. $\mathcal{A}_2$). Specifically, the defender and attacker respectively choose a mixed inspection strategy $\sigma^1 \in \Delta(\mathcal{A}_1)$ and a mixed attack strategy $\sigma^2 \in \Delta(\mathcal{A}_2)$, where $\Delta(\mathcal{A}_1) \coloneqq \{\sigma^1 \in [0,1]^{|\mathcal{A}_1|} \mid \sum_{S \in \mathcal{A}_1} \sigma^1_S = 1\}$ and

$\Delta(\mathcal{A}_2) \coloneqq \{\sigma^2 \in [0,1]^{|\mathcal{A}_2|} \mid \sum_{T\in\mathcal{A}_2} \sigma^2_T = 1\}$ denote the strategy sets. Here, σ^1_S (resp. σ^2_T) represents the probability assigned to the detector positioning S (resp. attack plan T) by the defender's strategy σ^1 (resp. the attacker's strategy σ^2). The players' strategies are independent randomizations. Then, the expected players' payoffs for a mixed strategy profile $\sigma = (\sigma^1, \sigma^2) \in \Delta(\mathcal{A}_1) \times \Delta(\mathcal{A}_2)$ are given by:

$$U_1(\sigma^1, \sigma^2) = \mathbb{E}_\sigma \left[\mathrm{F}(S,T)\right], \tag{2.2}$$

$$U_2(\sigma^1, \sigma^2) = \mathbb{E}_\sigma \left[|T|\right] - \mathbb{E}_\sigma \left[\mathrm{F}(S,T)\right]. \tag{2.3}$$

We consider that each player faces a strategic uncertainty about the other player's action, but the model parameters $(\mathcal{G}, b_1, b_2)$ as well as the payoff functions and strategy sets are common knowledge. Thus, we arrive at the strategic game of complete information: $\Gamma(b_1, b_2) \coloneqq \langle\{1,2\}, (\Delta(\mathcal{A}_1), \Delta(\mathcal{A}_2)), (U_1, U_2)\rangle$, where we refer to the defender as player 1 (or **P1**) and the attacker as player 2 (or **P2**).

We illustrate this model with an example:

Example 1. Consider the network shown in Figure 2-1. In this network, critical components are represented by the edges of the graph, and detectors can be positioned on the vertices. Consider the detection model in which a detector positioned at any vertex can monitor edges at one hop vertically, and at two hops horizontally. Thus, $\mathcal{C}_{i_1} = \{e_1, e_2, e_3\}$, $\mathcal{C}_{i_2} = \{e_1, e_2, e_4\}$, $\mathcal{C}_{i_3} = \{e_1, e_2, e_5\}$, $\mathcal{C}_{i_4} = \{e_4, e_6, e_7\}$, $\mathcal{C}_{i_5} = \{e_5, e_6, e_8\}$, $\mathcal{C}_{i_6} = \{e_3, e_9, e_{10}\}$, $\mathcal{C}_{i_7} = \{e_7, e_9, e_{10}\}$, and $\mathcal{C}_{i_8} = \{e_8, e_9, e_{10}\}$.

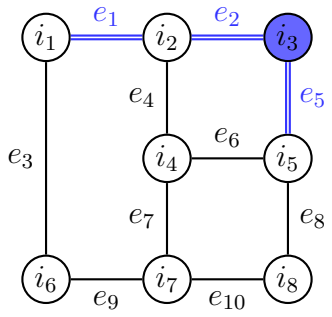
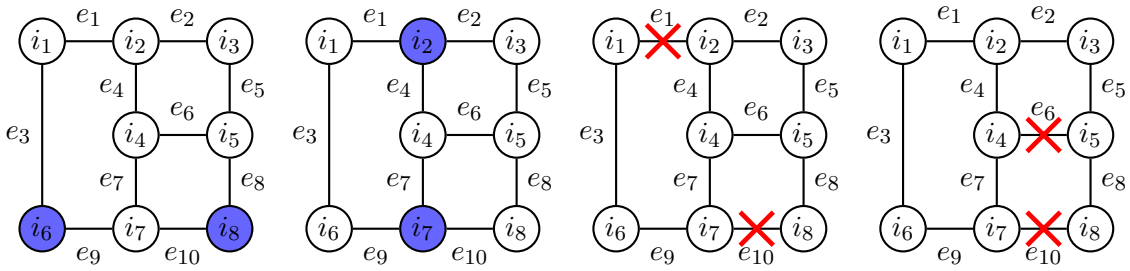


Figure 2-1: Example network. The monitoring set $\mathcal{C}_{i_3} = \{e_1, e_2, e_5\}$ is represented by the double blue edges.

P1 has $b_1 = 2$ detectors that she positions according to the inspection strategy

σ^1 defined by $\sigma^1_{\{i_6,i_8\}} = \frac{1}{4}$ and $\sigma^1_{\{i_2,i_7\}} = \frac{3}{4}$. Similarly, **P2** has $b_2 = 2$ attack resources that she allocates according to the attack strategy σ^2 defined by $\sigma^2_{\{e_1,e_{10}\}} = \frac{1}{2}$ and $\sigma^2_{\{e_6,e_{10}\}} = \frac{1}{2}$. The strategy profile (σ^1, σ^2) is illustrated in Figure 2-2. Since $\mathrm{F}(\{i_6, i_8\}, \{e_1, e_{10}\}) = 1$, $\mathrm{F}(\{i_6, i_8\}, \{e_6, e_{10}\}) = 1$, $\mathrm{F}(\{i_2, i_7\}, \{e_1, e_{10}\}) = 2$, and $\mathrm{F}(\{i_2, i_7\}, \{e_6, e_{10}\}) = 1$, then **P1**'s expected payoff is $U_1(\sigma^1, \sigma^2) = \frac{11}{8}$ and **P2**'s expected payoff is $U_2(\sigma^1, \sigma^2) = \frac{5}{8}$.



(a) $\sigma^1_{\{i_6,i_8\}} = \frac{1}{4}$. (b) $\sigma^1_{\{i_2,i_7\}} = \frac{3}{4}$. (c) $\sigma^2_{\{e_1,e_{10}\}} = \frac{1}{2}$. (d) $\sigma^2_{\{e_6,e_{10}\}} = \frac{1}{2}$.

Figure 2-2: **P1**'s inspection strategy σ^1 (left) and **P2**'s attack strategy σ^2 (right) for the example network in Figure 2-1.

△

A strategy profile $(\sigma^{1*}, \sigma^{2*}) \in \Delta(\mathcal{A}_1) \times \Delta(\mathcal{A}_2)$ is a mixed strategy *Nash Equilibrium* (NE) of the game $\Gamma(b_1, b_2)$ if:

$$\forall \sigma^1 \in \Delta(\mathcal{A}_1),\ U_1(\sigma^{1*}, \sigma^{2*}) \geq U_1(\sigma^1, \sigma^{2*}), \tag{2.4}$$

$$\forall \sigma^2 \in \Delta(\mathcal{A}_2),\ U_2(\sigma^{1*}, \sigma^{2*}) \geq U_2(\sigma^{1*}, \sigma^2). \tag{2.5}$$

Furthermore, given $\epsilon \geq 0$, a strategy profile $(\sigma^{1\prime}, \sigma^{2\prime}) \in \Delta(\mathcal{A}_1) \times \Delta(\mathcal{A}_2)$ is an $\epsilon-NE$ if:

$$\forall \sigma^1 \in \Delta(\mathcal{A}_1),\ U_1(\sigma^{1\prime}, \sigma^{2\prime}) \geq U_1(\sigma^1, \sigma^{2\prime}) - \epsilon, \tag{2.6}$$

$$\forall \sigma^2 \in \Delta(\mathcal{A}_2),\ U_2(\sigma^{1\prime}, \sigma^{2\prime}) \geq U_2(\sigma^{1\prime}, \sigma^2) - \epsilon. \tag{2.7}$$

We denote the set of NE (resp. set of $\epsilon-$NE) of the game $\Gamma(b_1, b_2)$ as $\Sigma(b_1, b_2)$ (resp. $\Sigma_\epsilon(b_1, b_2)$).

From a game-theoretic viewpoint, a NE in mixed strategies describes the behavior of **P1** and **P2** who play the game Γ repeatedly against each other and ignore any strategic relationship in-between plays. In such a repeated play, each player cannot guess the actions of her opponent in any particular round of play [35]. Thus, NE in mixed strategies can be viewed as a stochastic steady state of the repeated interaction between players. By extension, we view $\epsilon-$NE as strategy profiles in which the players are almost at a stochastic steady state, i.e., no player has more than an incentive of ϵ to change her mixed strategy.

For ease of exposition, we denote $\mathrm{F}(i,e) \coloneqq \mathrm{F}(\{i\},\{e\}),\ \forall (i,e) \in \mathcal{V} \times \mathcal{E}$. We will also use the notations $U_i(S,\sigma^2) = U_i(\mathbb{1}_{\{S\}},\sigma^2)$ and $U_i(\sigma^1,T) = U_i(\sigma^1,\mathbb{1}_{\{T\}})$ for $i \in \{1,2\}$. The *support* of $\sigma^1 \in \Delta(\mathcal{A}_1)$ (resp. $\sigma^2 \in \Delta(\mathcal{A}_2)$) is defined as $\mathrm{supp}(\sigma^1) = \{S \in \mathcal{A}_1 \mid \sigma^1_S > 0\}$ (resp. $\mathrm{supp}(\sigma^2) = \{T \in \mathcal{A}_2 \mid \sigma^2_T > 0\}$). The *node basis* of a strategy $\sigma^1 \in \Delta(\mathcal{A}_1)$, denoted $\mathcal{V}_{\sigma^1} \coloneqq \{i \in \mathcal{V} \mid \mathbb{P}_{\sigma^1}(i \in S) > 0\}$, is the set of nodes that are inspected with non-zero probability. Analogously, the *component basis* of a strategy $\sigma^2 \in \Delta(\mathcal{A}_2)$, denoted $\mathcal{E}_{\sigma^2} \coloneqq \{e \in \mathcal{E} \mid \mathbb{P}_{\sigma^2}(e \in T) > 0\}$, is the set of components that are targeted with positive probability. Also, when there is no confusion, we will refer to $\Gamma(b_1,b_2)$, $\Sigma(b_1,b_2)$, and $\Sigma_\epsilon(b_1,b_2)$ simply as Γ, Σ, and Σ_ϵ.

Henceforth, we assume without loss of generality that each component in $\mathcal{E}$ can be monitored from at least one node in $\mathcal{V}$. Indeed, if k components cannot be monitored from any node in the network, then **P2**'s incentive is to always target those components, and then allocate her remaining resources (if any) to target other components. We can remove those k components from $\mathcal{E}$, and solve the resulting game where **P2** now has $\max\{b_2-k,0\}$ resources that she can allocate on the resulting subnetwork (where each component is now monitored from at least one node); we simply need to increase her payoff by $\min\{k,b_2\}$ to account for the components already targeted and never detected by **P1**.

Despite its simplicity, the game $\Gamma(b_1,b_2)$ captures some of the key features of network inspection in strategic settings, as listed in Table 2.2.

Firstly, the underlying detection model $\mathcal{G}$ is generic in that it represents the detection capability of the defender, without making further modeling assumptions about

Table 2.2: List of applications of our network inspection problem.

Inspection setting	Network	Type of detector	Type of attacks
Urban patrolling	City streets	Police unit	Robbery
Network security	Information network	Firewall	Cyberattack on server
Sensing of gas and water networks	Gas and water pipelines	Leak/pressure sensor	Pipe disruption
Interdiction of illegal goods	Transportation network	Police officer	Drug trafficking
Infiltration game	Water channel	Electric cable	Malicious infiltration

how the monitoring sets $\mathcal{C}_i$, $i \in \mathcal{V}$, depend on specific aspects such as sensing technology employed by the detectors, the different means that the attacker may use in targeting a component, and the network's topological structure [5, 95, 97]. Secondly, it considers multiple resources on the part of both defender and attacker. This is a particularly desirable feature for strategic inspection settings, in which the attacker can simultaneously attack multiple components across the network, and the defender's inspection involves positioning multiple detectors in order to monitor a large number of critical components. In contrast, the previously studied security games typically assume that one or both players are constrained to using only a single resource; see Table 2.1.

More importantly, any strategy profile of the game $\Gamma(b_1, b_2)$ can be associated with a metric of detection performance against attacks. For a given strategy profile $\sigma \in \Delta(\mathcal{A}_1) \times \Delta(\mathcal{A}_2)$, we define this metric as the *expected detection rate*, $r(\sigma)$, which is the expectation (under σ) of the ratio between the number of attacks that are detected and the total number of attacks:

$$r(\sigma) \coloneqq \mathbb{E}_\sigma \left[\frac{\mathrm{F}(S,T)}{|T|} \right]. \tag{2.8}$$

We are now in the position to introduce our network inspection problem, which we define as a mathematical program with equilibrium constraints. In this problem, given the attacker's resources b_2, the defender seeks to determine a minimum-resource inspection strategy (i.e., to minimize the number of detectors b_1 and strategically position them in the network), while ensuring that the expected detection rate in

any equilibrium of the game $\Gamma(b_1, b_2)$ is no less than a pre-specified threshold level $\alpha \in [0, 1]$:

$$
\begin{aligned}
(\mathcal{P}): \quad & \underset{b_1,\, \sigma^\dagger}{\text{minimize}} && b_1 \\
& \text{subject to} && r(\sigma^*) \geq \alpha, \qquad \forall \sigma^* \in \Sigma(b_1, b_2) && (2.9) \\
& && \sigma^\dagger \in \Sigma(b_1, b_2) && (2.10) \\
& && b_1 \in \mathbb{N}.
\end{aligned}
$$

Constraints (2.9) ensure that the expected detection rate in any equilibrium of the game induced by the chosen number of detectors b_1 and the given number of attack resources b_2 is at least α. Constraint (2.10) requires the computation of one NE of game $\Gamma(b_1, b_2)$, which exists due to Nash's Theorem [78]. The optimal value of $(\mathcal{P})$, denoted $b_1^\dagger$, is the minimum number detectors for which the equilibrium constraints (2.9)-(2.10) are satisfied. Thus, $(b_1^\dagger, \sigma^\dagger)$ with $\sigma^\dagger \in \Sigma(b_1^\dagger, b_2)$ is an optimal solution of $(\mathcal{P})$, where the inspection strategy in $\sigma^\dagger$ specifies a randomized positioning of $b_1^\dagger$ detectors. The target detection rate α reflects the performance requirement that the defender seeks to achieve in any equilibrium of the game, besides seeking a minimum-resource inspection strategy.

2.3 Equilibrium Strategies

To solve the inspection problem $(\mathcal{P})$ in a brute force manner, one would need to compute every NE of the game $\Gamma(b_1, b_2)$ for each $b_1 \in \mathbb{N}$, and check – for each of them – whether or not the expected detection rate is at least α. Clearly, this exhaustive approach is not computationally scalable. One way to approach this problem is to note that Γ is strategically equivalent to the zero-sum game $\widetilde{\Gamma} := \langle \{1, 2\}, (\Delta(\mathcal{A}_1), \Delta(\mathcal{A}_2)), (-U_2, U_2) \rangle$. Therefore, the NE of Γ can be obtained by solving the following two linear programming problems:

$$
(\text{LP}_1) \quad \max_{\sigma^1 \in \Delta(\mathcal{A}_1)} \min_{T \in \mathcal{A}_2} -U_2(\sigma^1, T) \qquad \Big| \qquad (\text{LP}_2) \quad \max_{\sigma^2 \in \Delta(\mathcal{A}_2)} \min_{S \in \mathcal{A}_1} U_2(S, \sigma^2).
$$

Thus, in principle, linear programming techniques can be used to compute NE of Γ. However, the computation of (LP_1) and (LP_2) quickly becomes intractable as the size of the network increases. In particular, due to the size of the players' sets of actions ($|\mathcal{A}_1| = \sum_{k=0}^{b_1} \binom{|\mathcal{V}|}{k}$ and $|\mathcal{A}_2| = \sum_{l=0}^{b_2} \binom{|\mathcal{E}|}{l}$), the number of variables and constraints in both linear programs can be huge. For example, for a network consisting of 200 nodes and components, and $b_1 = b_2 = 10$, computing the equilibria of game $\Gamma(b_1, b_2)$ entails solving linear programs containing $2.37 \cdot 10^{16}$ variables and constraints. For large bimatrix games, Lipton et al. [69] provide an algorithm to compute an $\epsilon-$NE in $n^{O(\ln n/\epsilon^2)}$ time. However, for realistic instances of the game Γ, the number of available pure strategies n for each player can easily reach values for which the algorithm is practically inapplicable.

In this section, we develop new results to study the equilibrium characteristics of the game $\Gamma(b_1, b_2)$, given any parameters b_1 and b_2. Our equilibrium characterization utilizes properties of two combinatorial optimization problems, formulated as minimum set cover and maximum set packing problems. We also construct an approximate NE using solutions of these problems and derive bounds on the detection performance, which subsequently enable us to solve the network inspection problem ($\mathcal{P}$).

2.3.1 Set Cover and Set Packing Problems

We say that a set of nodes $S \in 2^{\mathcal{V}}$ is a *set cover* if and only if every component in $\mathcal{E}$ can be monitored by at least one detector positioned in S, i.e., $\mathrm{F}(S, e) = 1$, $\forall e \in \mathcal{E}$. A set of nodes $S \in 2^{\mathcal{V}}$ is a *minimal set cover* if S is a set cover that is minimum with respect to inclusion, i.e., if any node of S is removed, the resulting set is not a set cover anymore. A set of nodes $S \in 2^{\mathcal{V}}$ is a *minimum set cover* (MSC) if and only if it is an optimal solution of the following problem:

$$(\mathcal{I}_{\mathrm{MSC}}): \underset{S \in 2^{\mathcal{V}}}{\text{minimize}} \ |S| \quad \text{subject to} \quad \mathrm{F}(S, e) = 1, \quad \forall e \in \mathcal{E}. \tag{2.11}$$

Solving ($\mathcal{I}_{\mathrm{MSC}}$) amounts to determining the minimum number of detectors and

their positioning to monitor all network components. We denote the set (resp. the size) of MSCs by $\mathcal{S}$ (resp. n^*). Since we assumed that each component can be monitored from at least one node in the network (Section 2.2.2), ($\mathcal{I}_{\text{MSC}}$) is feasible and n^* exists.

We say that a set of components $T \in 2^{\mathcal{E}}$ is a *set packing* if and only if a detector positioned at any node i can monitor at most one component in T, i.e., $\text{F}(i,T) \leq 1,\ \forall i \in \mathcal{V}$. A set of components $T \in 2^{\mathcal{E}}$ is a *maximum set packing* (MSP) if and only if it optimally solves the following problem:

$$(\mathcal{I}_{\text{MSP}}) : \underset{T \in 2^{\mathcal{E}}}{\text{maximize}}\ |T| \quad \text{subject to} \quad \text{F}(i,T) \leq 1, \quad \forall i \in \mathcal{V}. \tag{2.12}$$

Solving ($\mathcal{I}_{\text{MSP}}$) amounts to finding the maximum number of "independent" components, i.e., a set of components of maximum size such that monitoring each component requires a unique detector. We denote the set (resp. the size) of MSPs by $\mathcal{M}$ (resp. m^*).

To formulate ($\mathcal{I}_{\text{MSC}}$) and ($\mathcal{I}_{\text{MSP}}$) as integer programs, we define the *detection matrix* $\boldsymbol{F} = (\text{F}(i,e))_{(i,e)\in\mathcal{V}\times\mathcal{E}}$. $\boldsymbol{F}$ is a $|\mathcal{V}| \times |\mathcal{E}|$ binary matrix whose rows (resp. columns) are indexed by the nodes (resp. components) in the network. Thus, a given row of $\boldsymbol{F}$ indicates the components of the network that a detector positioned at the corresponding node monitors. Similarly, a given column of $\boldsymbol{F}$ indicates the locations from where a detector is capable of monitoring the corresponding component.

Then, solving ($\mathcal{I}_{\text{MSC}}$) is equivalent to selecting a subset of rows of the detection matrix $\boldsymbol{F}$ of minimum cardinality such that each column of $\boldsymbol{F}$ is covered, i.e., it has at least one 1 entry in the selected subset of rows. This problem can be formulated as the following integer program:

$$\begin{aligned} \text{minimize} \quad & \mathbf{1}_{|\mathcal{V}|}^{\top} x \\ \text{subject to} \quad & \boldsymbol{F}^{\top} x \geq \mathbf{1}_{|\mathcal{E}|} \\ & x \in \{0,1\}^{|\mathcal{V}|}, \end{aligned} \tag{2.13}$$

where $\mathbf{1}_{|\mathcal{V}|}$ (resp. $\mathbf{1}_{|\mathcal{E}|}$) represents the vector of length $|\mathcal{V}|$ (resp. $|\mathcal{E}|$) filled with ones.

Similarly, solving $(\mathcal{I}_{\text{MSP}})$ is equivalent to selecting a subset of columns of $\boldsymbol{F}$ of maximum cardinality such that each row of $\boldsymbol{F}$ has at most one 1 entry in the selected subset of columns:

$$\begin{aligned} \text{maximize} \quad & \mathbf{1}_{|\mathcal{E}|}^{\top} y \\ \text{subject to} \quad & \boldsymbol{F} y \leq \mathbf{1}_{|\mathcal{V}|} \\ & y \in \{0,1\}^{|\mathcal{E}|}. \end{aligned} \tag{2.14}$$

We illustrate $(\mathcal{I}_{\text{MSC}})$ and $(\mathcal{I}_{\text{MSP}})$ with the following example:

Example 2. Consider the detection model represented in Figure 2-1. Then, the corresponding detection matrix is given by:

$$\boldsymbol{F} = \begin{array}{c} \\ i_1 \\ i_2 \\ i_3 \\ i_4 \\ i_5 \\ i_6 \\ i_7 \\ i_8 \end{array} \begin{array}{c} \begin{array}{cccccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 & e_{10} \end{array} \\ \left(\begin{array}{cccccccccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array} \right) \end{array}.$$

Then, a solution of $(\mathcal{I}_{\text{MSC}})$ is given by $\{i_3, i_4, i_6, i_8\}$ and a solution of $(\mathcal{I}_{\text{MSP}})$ is given by $\{e_3, e_4, e_8\}$. They are illustrated in Figure 2-3.

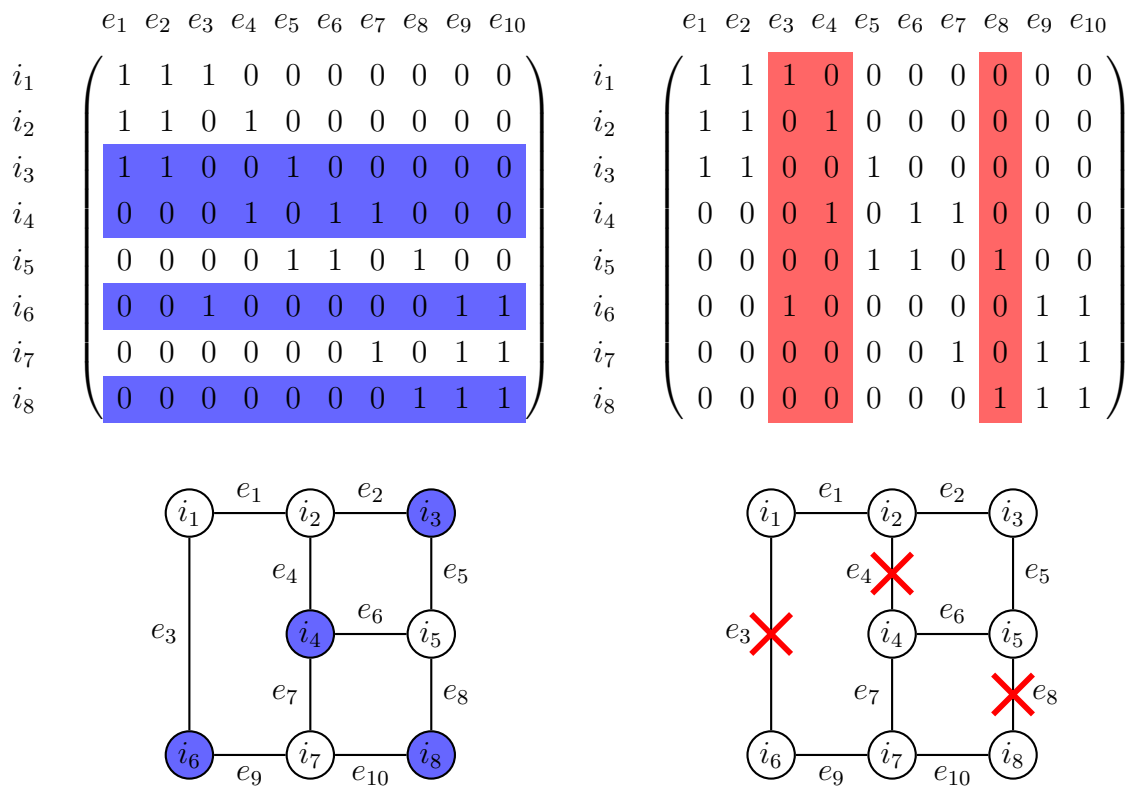


Figure 2-3: Illustration of an MSC (left) and an MSP (right) on the detection matrix (top) and the network (bottom) corresponding to the detection model in Figure 2-1.

△

Although ($\mathcal{I}_{\text{MSC}}$) and ($\mathcal{I}_{\text{MSP}}$) are known to be NP-hard problems [106], modern mixed-integer optimization solvers can be used to optimally solve them for realistic problem instances; see Section 2.5. Furthermore, their integer programming formulations (see (2.13)-(2.14)) have linear programming relaxations that are dual of each other. This implies that $m^* \leq n^*$.

MSCs and MSPs naturally arise in our approach for equilibrium characterization due to the fact that they provide a measure of *coverage* and *spread* of the network: n^* represents the minimum number of detectors required by **P1** to completely monitor the network, and m^* represents the maximum number of attack resources for which **P2** can spread her attacks across the network. In fact, solving $\Gamma(b_1, b_2)$ is trivial when $b_1 \geq n^*$, because **P1** can monitor all network components by deterministically

positioning the detectors on an MSC. A direct consequence is that the optimal number of detectors in $(\mathcal{P})$, $b_1^\dagger$, is at most n^*.

Additionally, the equilibrium characterization of the game $\Gamma(b_1, b_2)$ is practically relevant (and interesting) when **P2**'s number of attack resources is less than the size of MSPs, i.e., $b_2 < m^*$. This case captures the situations in which the network is "large enough" in that **P2** can exhaust her ability to spread attacks, thereby making it most challenging for **P1** to detect the attacks using her inspection strategy. Furthermore, when $b_2 \geq m^*$, a larger number of attack resources improves **P1**'s ability to detect some of the attacks. Thus, an inspection strategy that ensures the target detection performance for the case $b_2 < m^*$ can also be applied when $b_2 \geq m^*$ (see Section 2.8.1). Henceforth, our analysis of the game $\Gamma(b_1, b_2)$ primarily focuses on the case when $b_1 < n^*$ and $b_2 < m^*$ (see Figure 2-4). We discuss the other cases whenever relevant.

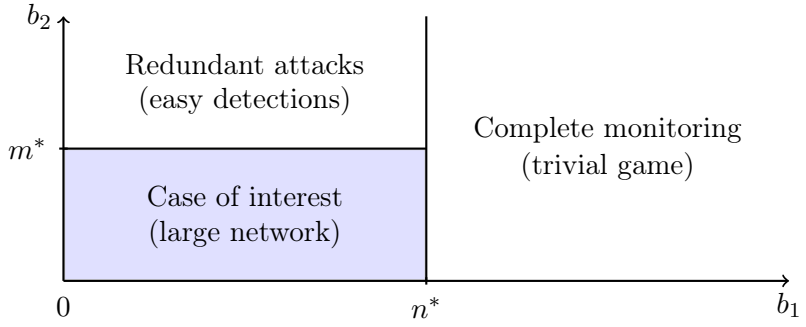


Figure 2-4: Equilibrium regimes with respect to the players' resources b_1 and b_2.

2.3.2 Equilibrium Properties

Our analysis of the game $\Gamma(b_1, b_2)$ proceeds in three steps: Firstly, we derive bounds on the players' equilibrium payoffs in the strategically equivalent zero-sum game $\widetilde{\Gamma}(b_1, b_2)$ (Proposition 1). Secondly, we show that every NE satisfies certain structural properties, which enables us to obtain bounds on the players' payoffs and the expected detection rate in equilibirium of the original game $\Gamma(b_1, b_2)$ (Propositions 2-3 and Theorem 1). Finally, we construct an approximate NE based on exact or approximate solutions to the MSC and MSP problems (Theorem 2).

Recall that in any equilibrium, **P1**'s strategy is an optimal solution of (LP_1), and **P2**'s strategy is an optimal solution of (LP_2). Moreover, the optimal values of these linear programs represent the players' equilibrium payoffs in the game $\widetilde{\Gamma}(b_1, b_2)$. In the first step of our analysis, we derive bounds on the optimal values of (LP_1) and (LP_2), along with mixed strategies that achieve these bounds. To carry out this step, we utilize the following construction of a mixed strategy profile: consider a set of nodes S of size at least b_1 and a set of components T of size at least b_2. Lemma 1 below shows the existence of a mixed strategy profile whose node basis and component basis (as defined in Section 2.2.2) are S and T respectively, and which satisfies the following properties: (a) **P1** randomizes the positioning of her detectors over subsets of S of size b_1 such that each node of S is inspected with an identical probability; (b) **P2** randomizes the attack of b_2 components in T such that each component is targeted with an identical probability.

Lemma 1. *Consider a set of nodes $S \in 2^{\mathcal{V}}$ of size $n \geq b_1$, and a set of components $T \in 2^{\mathcal{E}}$ of size $m \geq b_2$. Then, there exists a strategy profile, denoted $(\sigma^1(S, b_1), \sigma^2(T, b_2)) \in \Delta(\mathcal{A}_1) \times \Delta(\mathcal{A}_2)$, whose node basis and component basis are S and T respectively, and such that:*

$$\forall i \in S,\ \mathbb{P}_{\sigma^1(S,b_1)}(i \textit{ is inspected by } \textbf{\textit{P1}}) = \frac{b_1}{n}, \tag{2.15}$$

$$\forall e \in T,\ \mathbb{P}_{\sigma^2(T,b_2)}(e \textit{ is targeted by } \textbf{\textit{P2}}) = \frac{b_2}{m}. \tag{2.16}$$

For details on the construction of $(\sigma^1(S, b_1), \sigma^2(T, b_2))$, we refer to Lemma 6. The main idea behind the construction of the inspection strategy $\sigma^1(S, b_1)$ is to "cycle" over size-b_1 subsets of S, such that every node of S is inspected with an identical probability given by (2.15); similarly for the attack strategy $\sigma^2(T, b_2)$.

We illustrate this construction with an example:

Example 3. Consider a set of three nodes $S = \{i_1, i_2, i_3\}$ and suppose that **P1** has two detectors ($b_1 = 2$). First, we define three pure actions $S^1 = \{i_1, i_2\}$, $S^2 = \{i_2, i_3\}$, and $S^3 = \{i_3, i_1\}$; see Figure 2-5. The strategy $\sigma^1(S, b_1)$ is then obtained by assigning

uniform probability (i.e., $\frac{1}{3}$) to each pure action. One can check that each node in S is inspected with probability $\frac{2}{3} = \frac{b_1}{|S|}$.

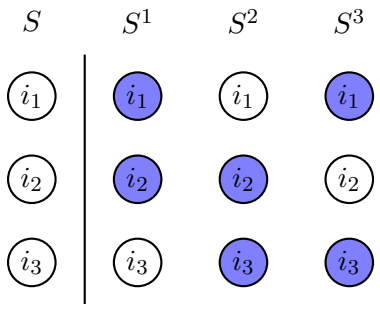


Figure 2-5: Support of $\sigma^1(S, b_1)$ when S is composed of three nodes and $b_1 = 2$.

△

Next, we use Lemma 1 to solve restricted versions of (LP_1) and (LP_2), where only specific subsets of variables are considered. Formally, given a subset of nodes $S' \in 2^{\mathcal{V}}$, and a subset of components $T' \in 2^{\mathcal{E}}$, consider the following linear programs:

$$(\text{LP}_{S'}) \quad \max_{\{\sigma^1 \in \Delta(\mathcal{A}_1) \,|\, \mathcal{V}_{\sigma^1} \subseteq S'\}} \min_{T \in \mathcal{A}_2} -U_2(\sigma^1, T)$$

$$(\text{LP}_{T'}) \quad \max_{\{\sigma^2 \in \Delta(\mathcal{A}_2) \,|\, \mathcal{E}_{\sigma^2} \subseteq T'\}} \min_{S \in \mathcal{A}_1} U_2(S, \sigma^2).$$

We note that adding the constraint $\mathcal{V}_{\sigma^1} \subseteq S'$ is equivalent to setting $\sigma^1_S = 0$ for every detector positioning S that contains a node outside of the set S'. It is easy to argue that the optimal values of ($\text{LP}_{S'}$) and ($\text{LP}_{T'}$) are lower bounds on **P1** and **P2**'s equilibrium payoffs in the zero-sum game $\widetilde{\Gamma}$. Furthermore, when S' and T' are the node basis and component basis of a NE, the optimal values of ($\text{LP}_{S'}$) and ($\text{LP}_{T'}$) are exactly equal to **P1** and **P2**'s equilibrium payoffs in $\widetilde{\Gamma}$.

We now discuss how to select a subset of nodes S' and a subset of components T' such that the optimal values of ($\text{LP}_{S'}$) and ($\text{LP}_{T'}$) are close to the players' equilibrium payoffs in the game $\widetilde{\Gamma}$. Recall that if **P1** had at least n^* detectors (i.e., $b_1 \geq n^*$), an equilibrium inspection strategy would be to position n^* detectors on an MSC. We claim that, even for the case when **P1** has strictly less than n^* detectors, a set cover is a good candidate for node basis. Analogously, a good candidate for component basis

is a set packing. Indeed, if **P2** targets components that are spread apart, then it will be difficult for the resource-constrained **P1** to detect many of these attacks. Thus, by targeting a set packing, **P2** can ensure that a single detector can detect at most one attack. In fact, when S' is a minimal set cover and T' is a set packing of size at least b_2, we can use the construction of the strategy profile $(\sigma^1(S', b_1), \sigma^2(T', b_2))$ in Lemma 1 to analytically solve $(\mathrm{LP}_{S'})$ and $(\mathrm{LP}_{T'})$.

Proposition 1. *Given a minimal set cover $S' \in 2^{\mathcal{V}}$, the optimal value of $(LP_{S'})$ is $b_2\left(\frac{b_1}{|S'|} - 1\right)$, and an optimal solution is given by $\sigma^1(S', b_1)$. Also, given a set packing $T' \in 2^{\mathcal{E}}$ of size at least b_2, the optimal value of $(LP_{T'})$ is $\max\left\{0, b_2\left(1 - \frac{b_1}{|T'|}\right)\right\}$, and an optimal solution is given by $\sigma^2(T', b_2)$.*

From this proposition, we know that for any minimal set cover S' and any set packing T' of size at least b_2, lower bounds on **P1** and **P2**'s equilibrium payoffs in the zero-sum game $\widetilde{\Gamma}$ are given by $b_2\left(\frac{b_1}{|S'|} - 1\right)$ and $\max\left\{0, b_2\left(1 - \frac{b_1}{|T'|}\right)\right\}$, respectively. By decreasing the size of the minimal set cover and increasing the size of the set packing, one can maximize the respective lower bounds. Thus, the best lower bound on the optimal value of (LP_1) (resp. (LP_2)) that we obtain is $b_2\left(\frac{b_1}{n^*} - 1\right)$ (resp. $\max\left\{0, b_2\left(1 - \frac{b_1}{m^*}\right)\right\}$). This concludes the first step of our analysis.

The second step consists of deriving structural properties satisfied by every NE. This enables us to translate the bounds on the players' equilibrium payoffs in game $\widetilde{\Gamma}$ to bounds on the expected equilibrium detection rate. An important property is that when $b_1 < n^*$ and $b_2 < m^*$, *any* equilibrium strategy for each player necessarily randomizes over actions that use all available resources.

Proposition 2. *In equilibrium, **P1** must choose an inspection strategy that randomizes over detector positionings of size exactly b_1, and **P2** must randomize her attacks over sets of b_2 components.*

$$\forall(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma,\ \forall S \in \mathrm{supp}(\sigma^{1^*}),\ |S| = b_1, \tag{2.17}$$

$$\forall(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma,\ \forall T \in \mathrm{supp}(\sigma^{2^*}),\ |T| = b_2. \tag{2.18}$$

Then, the NE of Γ *can be obtained by solving the following two linear programs:*

$$(\overline{LP_1}) \quad \max_{\sigma^1 \in \Delta(\overline{\mathcal{A}_1})} \min_{T \in \overline{\mathcal{A}_2}} U_1(\sigma^1, T) \qquad \Big| \qquad (\overline{LP_2}) \quad \min_{\sigma^2 \in \Delta(\overline{\mathcal{A}_2})} \max_{S \in \overline{\mathcal{A}_1}} U_1(S, \sigma^2)$$

where $\overline{\mathcal{A}_1} \coloneqq \{S \in 2^{\mathcal{V}} \mid |S| = b_1\}$ *and* $\overline{\mathcal{A}_2} \coloneqq \{T \in 2^{\mathcal{E}} \mid |T| = b_2\}$.

Although it is intuitive that both players *should* use all available resources, the value of this result lies in the fact that both players *must necessarily* do so. Property (2.17) is proven by showing that any additional detector can be utilized by **P1** to strictly improve her payoff, which holds because the network is "large" (captured by the inequality $b_1 < n^*$). Similarly, property (2.18) is proven by showing that any additional attack resource can be used by **P2** to strictly improve her payoff. This argument combines the fact that **P1** cannot monitor all network components with a single detector positioning, and that **P2** can spread her attacks (since $b_2 < m^*$). In addition, showing (2.18) involves using the features of the detection function F, Proposition 1, and the properties of ($\mathcal{I}_{\text{MSC}}$) and ($\mathcal{I}_{\text{MSP}}$). Proposition 2 also holds when $b_1 < n^*$ and $b_2 = m^*$. However, counterexamples can be found when $b_1 \geq n^*$ or $b_2 > m^*$; see Section 2.8.1.

From (2.17) and (2.18), we conclude that the NE of the game Γ can be obtained by solving smaller linear programs. Indeed, the number of variables and constraints can be reduced from $1 + \sum_{k=0}^{b_1} \binom{|\mathcal{V}|}{k}$ and $1 + \sum_{l=0}^{b_2} \binom{|\mathcal{E}|}{l}$ for (LP_1), to $1 + \binom{|\mathcal{V}|}{b_1}$ and $1 + \binom{|\mathcal{E}|}{b_2}$ for ($\overline{\text{LP}_1}$); similar reduction applies between (LP_2) and ($\overline{\text{LP}_2}$). Although ($\overline{\text{LP}_1}$) and ($\overline{\text{LP}_2}$) can be used to compute NE for small-sized networks, this approach is not applicable to large-sized networks. For example, for a network where $|\mathcal{V}| = |\mathcal{E}| = 200$ and $b_1 = b_2 = 10$, the number of variables and constraints only drop from $2.37 \cdot 10^{16}$ for (LP_1) and (LP_2) to $2.25 \cdot 10^{16}$ for ($\overline{\text{LP}_1}$) and ($\overline{\text{LP}_2}$). Therefore, using ($\overline{\text{LP}_1}$) and ($\overline{\text{LP}_2}$) to compute the NE of Γ is still not scalable.

Hence, we continue our analysis by focusing on the node bases of inspection strategies in equilibrium, which represent the sets of nodes that are inspected with positive probability by **P1**.

Proposition 3. *In any NE* $(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma$*, the node basis* $\mathcal{V}_{\sigma^{1^*}}$ *is a set cover.*

Furthermore, both players must necessarily randomize their actions in equilibrium.

Equivalently, in any NE, **P1**'s strategy monitors every component with positive probability. This directly implies that **P1** must necessarily choose a randomized inspection strategy, since each detector positioning is of size at most $b_1 < n^*$. In fact, Proposition 3 shows that, due to her resource constraints, **P2** must also randomize her actions in equilibrium. The proof of this result is based on a best-response argument, and uses the fact that from any inspection strategy that leaves one or more components completely unmonitored, we can construct another strategy that strictly improves **P1**'s payoff. This argument is completed by repositioning some detectors and evaluating the resulting change in **P1**'s payoff, which involves exploiting the submodularity of the detection function F, the upper bound on **P1**'s equilibrium payoff in $\widetilde{\Gamma}$ (Proposition 1), and the fact that the players must use all resources in equilibrium (Proposition 2). Interestingly, this result may not hold when $b_2 \geq m^*$: In that case, **P2** may target components that are "close" to each other, which can result in **P1** leaving some components completely unmonitored to focus on the ones for which targeted attacks are easier to detect; see Section 2.8.1 for an example.

Proposition 3 is also a practically relevant result. Consider, for example, the setting where the pure strategies of **P1** consist of placing and operating a set of detectors on a subset of locations (nodes) of the network that need to be initially prepared for the installation of detectors. The node basis of an inspection strategy in equilibrium would give the locations that need to be prepared, and the probability distribution σ^1 can be interpreted as the random scheduling of b_1 detectors on subsets of these locations. To minimize the number of locations that need to be prepared, we need to find an inspection strategy in equilibrium whose node basis is of minimum size. From Proposition 3, we deduce that this number is at least n^*, i.e., the size of an MSC.

We can now combine the aforementioned equilibrium properties to derive parametric bounds on the players' payoffs and the expected detection rate in equilibrium, which is crucial for addressing the equilibrium constraints (2.9) in $(\mathcal{P})$.

Theorem 1. *For a given detection model $\mathcal{G}$, and the players' resources $b_1 < n^*$ and $b_2 < m^*$, the game $\Gamma(b_1, b_2)$ has the following properties:*

(i) Equilibrium payoffs of both players are constant and bounded as follows:

$$\forall(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma(b_1, b_2),\ \frac{b_1 b_2}{n^*} \leq U_1(\sigma^{1^*}, \sigma^{2^*}) \leq \min\left\{\frac{b_1 b_2}{m^*}, b_2\right\},$$
$$\forall(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma(b_1, b_2),\ \max\left\{0, b_2\left(1 - \frac{b_1}{m^*}\right)\right\} \leq U_2(\sigma^{1^*}, \sigma^{2^*}) \leq b_2\left(1 - \frac{b_1}{n^*}\right).$$

(ii) In any equilibrium, the expected detection rate is constant and bounded as follows:

$$\forall \sigma^* \in \Sigma(b_1, b_2), \quad \frac{b_1}{n^*} \leq r(\sigma^*) \leq \min\left\{\frac{b_1}{m^*}, 1\right\}.$$

Firstly, we note that the lower and upper bounds on **P1**'s equilibrium payoff are nondecreasing with respect to b_1 and b_2. The intuition is that the more detectors **P1** has, the more attacks she will be able to detect. Also, the more attack resources **P2** has, the more components she will target (due to Proposition 2); this results in more detections, since each component is monitored with positive probability in equilibrium (Proposition 3). Secondly, these bounds are also nonincreasing with respect to n^* and m^*. Indeed, as the network size becomes larger, both n^* and m^* increase because each monitoring set covers a smaller fraction of the network. Thus, it is more difficult for **P1** to detect attacks (with the same number of detectors) in larger-sized networks, reducing her detection performance. Similar conclusions can be drawn regarding the bounds on **P2**'s equilibrium payoff. Thirdly, the bounds on the expected detection rate in equilibrium are nondecreasing with **P1**'s resources (because she can detect more attacks), and are nonincreasing with respect to n^* and m^* (because **P2** can spread her attacks further apart). Importantly, these bounds *do not* depend on the attack resources b_2. This property will be further investigated in Section 2.7.

The final step of our analysis consists of constructing an approximate NE (as defined in (2.6)-(2.7)) to address the constraint (2.10) of $(\mathcal{P})$. In particular, we

combine Propositions 1 and 2 to show that the construction introduced in Lemma 1, based on an MSC and an MSP, is an approximate NE of Γ.

Theorem 2. *Consider a detection model $\mathcal{G}$, and the players' resources $b_1 < n^*$ and $b_2 < m^*$. Then, for any MSC $S^{min} \in \mathcal{S}$ and any MSP $T^{max} \in \mathcal{M}$, the strategy profile $(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2))$ satisfies the following properties:*

(i.a) $\quad (\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2)) \in \Sigma_\epsilon(b_1, b_2),$

(i.b) $\quad \forall (\sigma^{1^*}, \sigma^{2^*}) \in \Sigma(b_1, b_2),\ \forall i \in \{1, 2\}:$

$$|U_i(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2)) - U_i(\sigma^{1^*}, \sigma^{2^*})| \leq \epsilon,$$

where $\epsilon = b_1 b_2 \left(\frac{1}{\max\{b_1, m^*\}} - \frac{1}{n^*} \right)$.

Furthermore, given an MSC $S^{min} \in \mathcal{S}$, the expected detection rate by positioning b_1 detectors according to $\sigma^1(S^{min}, b_1)$ provides the following detection guarantee:

(ii) $\quad \forall (\sigma^{1^*}, \sigma^{2^*}) \in \Sigma(b_1, b_2):$

$$\min_{\sigma^2 \in \Delta(\mathcal{A}_2)} r(\sigma^1(S^{min}, b_1), \sigma^2) \;=\; \frac{b_1}{n^*} \;\geq\; \frac{\max\{b_1, m^*\}}{n^*} r(\sigma^{1^*}, \sigma^{2^*}).$$

Theorem 2 $(i.a)$ implies that by computing an MSC and an MSP, we can construct an $\epsilon-$NE where ϵ depends on the players' resources and on the sizes of MSCs and MSPs. Furthermore, from $(i.b)$, we conclude that this $\epsilon-$NE has the additional property that it provides both players payoffs that are $\epsilon-$close to their respective equilibrium payoffs. It is important to note that this is not a generic property of $\epsilon-$NE, but a consequence of Propositions 1 and 2. Thanks to this result, our approximate NE is obtained by direct construction (i.e., by solving the MSC and MSP problems), and not by iterative computation.

Furthermore, from Theorem 2 (ii), we know that by using $\sigma^1(S^{min}, b_1)$ as inspection strategy, **P1** is guaranteed an expected detection rate of at least $\frac{b_1}{n^*}$, regardless of the attack strategy chosen by **P2**. This result can be viewed as a worst-case guarantee; that is, if **P1** wants to ensure that the expected detection rate is at least $\frac{b_1}{n^*}$ even

in the worst-case attack scenario, she can guarantee this performance by choosing $\sigma^1(S^{min}, b_1)$ as her inspection strategy. In fact, the relative difference between the expected detection rate in equilibrium and when **P1** chooses $\sigma^1(S^{min}, b_1)$ is upper bounded by $1 - \frac{\max\{b_1, m^*\}}{n^*}$; we refer to this bound as the *relative loss of performance*.

We note that when n^* and m^* become closer to each other (or equivalently, as the duality gap between ($\mathcal{I}_{\text{MSC}}$) and ($\mathcal{I}_{\text{MSP}}$) decreases), the gap between the upper and lower bounds in Theorem 1 also becomes narrower, and $(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2))$ in Theorem 2 becomes closer to a NE. Next, we refine these results to the case when $n^* = m^*$, and also comment on how our work generalizes some of the prior results in the literature on security games.

2.3.3 Special Cases

We argued in Section 2.3.1 that the size of MSPs m^* is no more than the size of MSCs n^* for any detection model $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \{\mathcal{C}_i,\ i \in \mathcal{V}\})$. However, in some situations, MSCs and MSPs are of same size. For example, consider a bipartite graph where detectors can be placed on the vertices to monitor adjacent edges (i.e., one-hop detection model). In this setting, MSCs and MSPs respectively become minimum vertex covers and maximum matching, and are of the same size [60].

In such examples (that is, when $b_1 < n^*$, $b_2 < m^*$, and $n^* = m^*$), we can refine our results in Theorems 1 and 2, and obtain a rather complete equilibrium characterization of the game Γ based on MSCs and MSPs. First, from Theorem 1, we notice that when $n^* = m^*$, the upper and lower bounds on both players' payoffs and the expected detection rate in equilibrium become equal. This observation is documented in the following corollary:

Corollary 1 (of Theorem 1)**.** *Consider a detection model $\mathcal{G}$ and the players' resources $b_1 < n^*$ and $b_2 < m^*$. If $n^* = m^*$, then the game $\Gamma(b_1, b_2)$ has the following properties:*

(i) Equilibrium payoffs of both players are constant and given by:

$$\forall(\sigma^{1^*},\sigma^{2^*})\in\Sigma(b_1,b_2),\quad \begin{cases} U_1(\sigma^{1^*},\sigma^{2^*})=\dfrac{b_1b_2}{n^*},\\ U_2(\sigma^{1^*},\sigma^{2^*})=b_2\left(1-\dfrac{b_1}{n^*}\right). \end{cases} \tag{2.19}$$

(ii) In any equilibrium, the expected detection rate is constant and given by:

$$\forall\sigma^*\in\Sigma(b_1,b_2),\quad r(\sigma^*)=\frac{b_1}{n^*}. \tag{2.20}$$

Secondly, it is easy to see that ϵ given in Theorem 2 is equal to 0 when $n^*=m^*$, which implies that the strategy profile defined in Lemma 1 is a NE. In fact, we can obtain a sufficient *and* necessary condition for a strategy profile constructed over an MSC and MSP to be a NE.

Proposition 4. *If $n^*=m^*$, $b_1<n^*$, and $b_2<m^*$, then for any MSC $S^{min}\in\mathcal{S}$ and any MSP $T^{max}\in\mathcal{M}$, a strategy profile $(\sigma^{1^*},\sigma^{2^*})\in\Delta(\mathcal{A}_1)\times\Delta(\mathcal{A}_2)$ whose node basis is S^{min} and whose component basis is T^{max} is a NE if and only if:*

$$\begin{aligned} &\forall i\in S^{min},\quad \mathbb{P}_{\sigma^{1^*}}(i \text{ is inspected})=\frac{b_1}{n^*},\\ \text{and}\quad &\forall e\in T^{max},\quad \mathbb{P}_{\sigma^{2^*}}(e \text{ is targeted})=\frac{b_2}{n^*}. \end{aligned} \tag{2.21}$$

In other words, a strategy profile in which **P1** and **P2** randomize over subsets of an MSC and an MSP is a NE if and only if each node of the MSC is inspected with an identical probability, and each component of the MSP is targeted with an identical probability, given by (2.21). This result is relevant for practical settings where it is of interest to minimize the number of network locations that need to be prepared to receive a detector (represented in our model by the node basis). From Proposition 3, we deduced that at least n^* locations are needed, and from Proposition 4, we know that, when $n^*=m^*$, there exists an inspection strategy in equilibrium whose node basis is an MSC. Therefore, in this case, we conclude that the minimum number of locations that need to be prepared to receive a detector in equilibrium is exactly n^*;

these locations form an MSC, S^{min}, and can be inspected according to the strategy $\sigma^1(S^{min}, b_1)$.

Proposition 4 generalizes the equilibrium characterization of prior results on security games. Indeed, our MSC/MSP-based characterization of NE applies to any detection model for which the equality $n^* = m^*$ holds. In Table 2.1, we list some of the classical models that fall into this category, and compare their features with those of our game. The table highlights the flexibility of our detection model $\mathcal{G}$, and compares the combinatorial objects underlying our equilibrium characterization with their settings. Importantly, our results generalize the players' equilibrium strategies to the case where they have multiple resources.

We end our analysis of the case $n^* = m^*$ with a further characterization of the support of the NE of Γ. In particular, using MSCs and MSPs, we derive necessary conditions that are satisfied by every NE.

Proposition 5. *If $b_1 < n^*$, $b_2 < m^*$, and $n^* = m^*$, then the set of NE has the following properties:*

(i) In any NE, a node is inspected with positive probability only if it monitors exactly one component of any MSP:

$$\forall(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma,\ \forall i \in \mathcal{V}_{\sigma^{1^*}},\ \forall T^{max} \in \mathcal{M},\ \mathrm{F}(i, T^{max}) = 1.$$

Furthermore, in any NE, a detector positioning is chosen with positive probability only if each of its detectors monitors a different component of any MSP:

$$\forall(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma,\ \forall S \in \mathrm{supp}(\sigma^{1^*}),\ \forall T^{max} \in \mathcal{M},\ \forall e \in T^{max},\ \mathrm{F}(S, e) = \sum_{i \in S} \mathrm{F}(i, e).$$

(ii) In any NE, a component is targeted with positive probability only if it is monitored from a unique node of any MSC:

$$\forall(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma,\ \forall e \in \mathcal{E}_{\sigma^{2^*}},\ \forall S^{min} \in \mathcal{S},\ \exists!\, i \in S^{min} \mid \mathrm{F}(i, e) = 1.$$

In other words, if there exists at least one MSP, T^{max}, such that a node $i \in \mathcal{V}$ does not monitor any edge in T^{max}, then i is never inspected in equilibrium. Moreover, Proposition 5 tells us that if there exists a component $e \in \mathcal{E}$ of an MSP such that at least two detectors of a detector positioning S monitor e, then S is never chosen in equilibrium; since **P2** targets components that are spread across the network, **P1** must avoid redundant detections. Similarly, if there exists at least one MSC, S^{min}, such that a component e is monitored from at least two nodes in S^{min}, then e is never targeted in equilibrium.

2.4 Solving the Network Inspection Problem

In the previous section, we derived properties satisfied by all equilibrium inspection and attack strategies in the game $\Gamma(b_1, b_2)$, with $b_1 < n^*$ and $b_2 < m^*$. These properties enabled us to prove Theorem 1 which provides bounds on the expected detection rate in any NE, and also Theorem 2 which gives an $\epsilon-$NE of Γ using optimal solutions of $(\mathcal{I}_{\text{MSC}})$ and $(\mathcal{I}_{\text{MSP}})$. Next, we use these results to derive a solution approach to approximately solve the network inspection problem $(\mathcal{P})$.

To motivate our approach, let us first consider the special case of $n^* = m^*$. From (2.20), we can easily conclude that the minimum number of detectors that are needed for the expected detection rate to be at least α in equilibrium is $b_1^\dagger = \lceil \alpha n^* \rceil$. Besides, for an MSC S^{min} and an MSP T^{max}, we know from Proposition 4 that $(\sigma^1(S^{min}, b_1^\dagger), \sigma^2(T^{max}, b_2))$ is a NE of the game $\Gamma(b_1^\dagger, b_2)$. Therefore, when $b_2 < m^*$ and $n^* = m^*$, our approach straightforwardly provides an optimal solution of the network inspection problem $(\mathcal{P})$, given by $\lceil \alpha n^* \rceil$, $(\sigma^1(S^{min}, \lceil \alpha n^* \rceil), \sigma^2(T^{max}, b_2))$.

Now consider the problem $(\mathcal{P})$ in the general case $m^* \leq n^*$. *Can our approach be extended to obtain an approximate solution of $(\mathcal{P})$ in this general case?* To address this question, we consider $\epsilon-$NE as an admissible equilibrium concept for the game Γ, and focus on a relaxed version of $(\mathcal{P})$ in which the constraint (2.10) is replaced by $\sigma^\dagger \in \Sigma_\epsilon(b_1, b_2)$, with $\epsilon \geq 0$. Our next result shows that this relaxed problem, denoted $(\mathcal{P}_\epsilon)$, is approximately solvable using our approach.

Proposition 6. *Consider a detection model $\mathcal{G}$, a target detection performance $\alpha \in [0,1]$, and **P2**'s attack resources $b_2 < m^*$. Then, for any MSC $S^{min} \in \mathcal{S}$ and any MSP $T^{max} \in \mathcal{M}$, $b_1' \coloneqq \lceil \alpha n^* \rceil$ and $(\sigma^1(S^{min}, b_1'), \sigma^2(T^{max}, b_2))$ is an approximate solution of $(\mathcal{P}_\epsilon)$, where $\epsilon = b_1' b_2 \left(\frac{1}{\max\{b_1', m^*\}} - \frac{1}{n^*} \right)$, with an optimality gap given by $\lceil \alpha n^* \rceil - \lceil \alpha m^* \rceil$.*

Indeed, with $\lceil \alpha n^* \rceil$ detectors, the lower bound on the expected detection rate in equilibrium of the induced game $\Gamma(\lceil \alpha n^* \rceil, b_2)$, given in Theorem 1, ensures that the equilibrium constraints (2.9) are satisfied. Furthermore, the upper bound on the expected equilibrium detection rate in Theorem 1 implies that **P1** needs at least $\lceil \alpha m^* \rceil$ detectors to satisfy (2.9). Consequently, the optimal value of $(\mathcal{P}_\epsilon)$ satisfies $\lceil \alpha m^* \rceil \leq b_1^\dagger \leq \lceil \alpha n^* \rceil$, which gives the optimality gap in Proposition 6. Moreover, from Theorem 2, we know that our strategy profile constructed over an MSC and an MSP (according to Lemma 1) is an $\epsilon-$NE. Thus, we obtain an approximate solution of the relaxed problem $(\mathcal{P}_\epsilon)$, using solutions of the MSC and MSP problems. Clearly, this solution is optimal when $n^* = m^*$.

Next, we illustrate our solution approach with an example.

Example 4. Consider the network inspection problem $(\mathcal{P})$ for the detection model represented in Figure 2-1. The target expected detection rate is given by $\alpha = 0.75$, and the number of attack resources is $b_2 = 2$. For this small-sized problem, we can solve (LP_1) and (LP_2) to compute the NE of Γ, and obtain the expected detection rate in any NE for each $b_1 \in \mathbb{N}$. Table 2.3 summarizes the results.

Table 2.3: Expected detection rate in equilibrium for every $b_1 \in \mathbb{N}$.

b_1	0	1	2	3	≥ 4
$r(\sigma^*)$	0	$\frac{2}{7}$	$\frac{4}{7}$	$\frac{6}{7}$	1

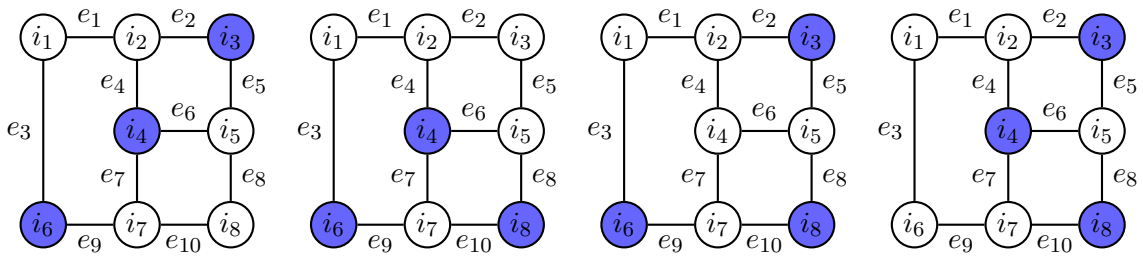
From Table 2.3, we conclude that the optimal value of $(\mathcal{P})$ is $b_1^\dagger = 3$, i.e., with 3 detectors, **P1** is capable of detecting $\frac{6}{7} \geq \alpha$ of the attacks in equilibrium. However, as mentioned in Section 2.3, this method does not extend to larger networks, as it requires solving large (LP_1) and (LP_2) for each $b_1 \in \mathbb{N}$ and checking if the constraints on the expected detection rate for every NE (2.9) are satisfied.

Now consider our solution approach based on the results presented in Sections 2.3 and 2.4: Firstly, by solving ($\mathcal{I}_{\text{MSC}}$), we obtain an MSC given by $S^{min} = \{i_3, i_4, i_6, i_8\}$; thus $n^* = 4$. Then, from Theorem 1, we know that the expected detection rate in any equilibrium of the game $\Gamma(b_1, b_2)$ is lower bounded by $\frac{b_1}{n^*}$. Thus, with $b_1' \coloneqq \lceil \alpha n^* \rceil = 3$ detectors, the expected detection rate in any equilibrium is at least α.

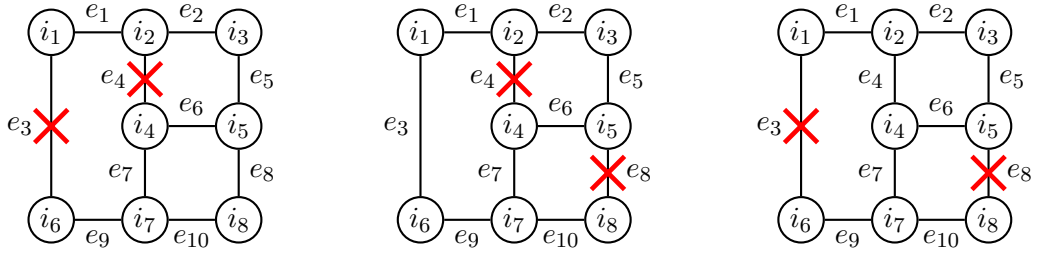
Secondly, by solving ($\mathcal{I}_{\text{MSP}}$), we obtain an MSP given by $T^{max} = \{e_3, e_4, e_8\}$; thus $m^* = 3$. Then, from Theorem 1, we know that the expected detection rate in any equilibrium of the game $\Gamma(b_1, b_2)$ is upper bounded by $\min\{\frac{b_1}{m^*}, 1\}$. This implies that if $b_1 < \lceil \alpha m^* \rceil$, then the equilibrium constraints (2.9) are not satisfied. Thus, an optimality gap associated with b_1' is given by $\lceil \alpha n^* \rceil - \lceil \alpha m^* \rceil$ (Proposition 6). In fact, for this example, we obtain that the optimality gap is $\lceil 3 \rceil - \lceil 2.25 \rceil = 0$. Therefore, by solving ($\mathcal{I}_{\text{MSC}}$) and ($\mathcal{I}_{\text{MSP}}$), we can estimate the number of detectors to ensure that the equilibrium constraints in ($\mathcal{P}$) are satisfied; furthermore, we can verify that this number is optimal for this example, i.e., $b_1' = b_1^\dagger = 3$.

Thirdly, given $b_1' = 3$ and $b_2 = 2$, we use S^{min} and T^{max} to construct an approximate NE. Using Lemma 1, we construct the strategy profile $\sigma = (\sigma^1, \sigma^2)$ defined by $\sigma^1_{\{i_3,i_4,i_6\}} = \sigma^1_{\{i_4,i_6,i_8\}} = \sigma^1_{\{i_6,i_8,i_3\}} = \sigma^1_{\{i_8,i_3,i_4\}} = \frac{1}{4}$, and $\sigma^2_{\{e_3,e_4\}} = \sigma^2_{\{e_4,e_8\}} = \sigma^2_{\{e_8,e_3\}} = \frac{1}{3}$; σ is illustrated in Figure 2-6. From Theorem 2, we obtain that the above-constructed strategy profile σ is an $\epsilon-$NE, and provides each player a payoff that is $\epsilon-$close to their equilibrium payoff, with $\epsilon = b_1' b_2 \left(\frac{1}{\max\{b_1', m^*\}} - \frac{1}{n^*} \right) = \frac{1}{2}$. Indeed, from ($\text{LP}_1$) and ($\text{LP}_2$), we can deduce that **P1** and **P2**'s equilibrium payoffs in the game Γ are $\frac{12}{7}$ and $\frac{2}{7}$ respectively, while our strategy profile σ provides them with the respective payoffs $\frac{3}{2}$ and $\frac{1}{2}$. One can easily check that σ gives each player a payoff that is $\frac{3}{14}$ ($\leq \epsilon$) close to their equilibrium payoff.

Finally, we give an upper bound on the relative loss of performance by choosing our inspection strategy σ^1 (see Figure 2-6 (top)), instead of choosing an equilibrium strategy for **P1**. From Theorem 2, we know that with 3 detectors, σ^1 detects at least $\frac{3}{4}$ of the attacks regardless of **P2**'s strategy. On the other hand, in equilibrium, $\frac{6}{7}$ of the attacks are detected (Table 2.3). Thus, the relative loss of performance is 12.5 %. This exact calculation is possible only because, for this example, we can solve (LP_1)



(a) $\sigma^1_{\{i_3,i_4,i_6\}} = \frac{1}{4}$. (b) $\sigma^1_{\{i_4,i_6,i_8\}} = \frac{1}{4}$. (c) $\sigma^1_{\{i_6,i_8,i_3\}} = \frac{1}{4}$. (d) $\sigma^1_{\{i_8,i_3,i_4\}} = \frac{1}{4}$.



(e) $\sigma^2_{\{e_3,e_4\}} = \frac{1}{3}$. (f) $\sigma^2_{\{e_4,e_8\}} = \frac{1}{3}$. (g) $\sigma^2_{\{e_8,e_3\}} = \frac{1}{3}$.

Figure 2-6: **P1**'s inspection strategy σ^1 (top) and **P2**'s attack strategy σ^2 (bottom) for the example network in Figure 2-1.

and (LP_2) and compute the value of the expected detection rate in equilibrium. In contrast, Theorem 2 provides an upper bound on the relative loss of performance *without* solving (LP_1) and (LP_2), but instead by computing n^* and m^* from (2.13) and (2.14). This upper bound is given by $1 - \frac{\max\{b_1', m^*\}}{n^*} = 25\,\%$. △

We now summarize the main advantages of our solution approach. Firstly, it reduces to a significant extent the size of the optimization problems that are involved in computing a solution. Indeed, recall that the number of variables and constraints of (LP_1) is equal to $1 + \sum_{k=0}^{b_1} \binom{|\mathcal{V}|}{k}$ and $1 + \sum_{l=0}^{b_2} \binom{|\mathcal{E}|}{l}$ respectively. On the other hand, the number of variables and constraints of ($\mathcal{I}_{\text{MSC}}$) is only $|\mathcal{V}|$ and $|\mathcal{E}|$, respectively; analogous comparisons can be made between (LP_2) and ($\mathcal{I}_{\text{MSP}}$). Again, for a network with $|\mathcal{V}| = |\mathcal{E}| = 200$ and $b_1 = b_2 = 10$, the number of variables and constraints is reduced from $2.37 \cdot 10^{16}$ for (LP_1) and (LP_2) to only 200 for ($\mathcal{I}_{\text{MSC}}$) and ($\mathcal{I}_{\text{MSP}}$).

Secondly, solving a single instance of ($\mathcal{I}_{\text{MSC}}$) and ($\mathcal{I}_{\text{MSP}}$) enables us to use our approach and derive a solution to problem ($\mathcal{P}$) for any attack resources b_2, and any target detection rate α. In contrast, recall from Section 2.3 that computing an optimal solution of ($\mathcal{P}$) using (LP_1) and (LP_2) requires solving them for each value of

b_1. Furthermore, **P2**'s amount of resources b_2 explicitly enters in the formulation of (LP_1) and (LP_2) as a parameter. On the contrary, in our approach, **P1** does not need to know the exact amount of attack resources b_2 to determine the number of detectors she needs and how to position them. Indeed, from Theorem 2, we know that with $\lceil \alpha n^* \rceil$ detectors that are positioned according to $\sigma^1(S^{min}, \lceil \alpha n^* \rceil)$, **P1** is guaranteed to meet the target detection rate α. Furthermore, as long as $b_2 < m^*$, the performance guarantees, and the optimality gap associated with our solution can directly be computed from n^* and m^*. In fact, we argue in Section 2.7 that if $b_2 < m^*$, then the optimal number of detectors in ($\mathcal{P}$) does not depend on b_2, and their positioning in equilibrium can be determined by considering $b_2 = 1$.

Finally, we note that while the above-mentioned results require computing an MSC and an MSP (both NP-hard problems), modern mixed-integer optimization solvers can be used to optimally solve them (see Section 2.5). However, for extremely large-sized problems, these solvers may not be able to solve ($\mathcal{I}_{\text{MSC}}$) and ($\mathcal{I}_{\text{MSP}}$) to optimality. Still, we can extend our results based only on the computation of a set cover and a set packing. Indeed, using a heuristic or greedy algorithm [2, 23], one can compute a set cover S'. Then, our arguments in Proposition 6 can be extended to conclude that with $\lceil \alpha |S'| \rceil$ detectors, the expected detection rate in any equilibrium of the induced game is at least α. We can also construct an inspection strategy $\sigma^1(S', \lceil \alpha |S'| \rceil)$, which ensures that the expected detection rate is at least α, regardless of **P2**'s strategy. Of course, **P1** would end up using more sensing resources than if she had been able to compute an MSC. Similarly, a set packing T' can be computed using a heuristic [47, 49]. Again, by suitably extending Proposition 6, we can obtain an optimality gap associated with $\lceil \alpha |S'| \rceil$ of $\lceil \alpha |S'| \rceil - \lceil \alpha |T'| \rceil$. Finally, if T' is of size at least b_2, we can also conclude that $(\sigma^1(S', \lceil \alpha |S'| \rceil), \sigma^2(T', b_2))$ is an $\tilde{\epsilon}-$NE, where $\tilde{\epsilon} = \lceil \alpha |S'| \rceil b_2 \left(\frac{1}{\max\{\lceil \alpha |S'| \rceil, |T'|\}} - \frac{1}{|S'|} \right)$; this $\tilde{\epsilon}-$NE provides each player a payoff that is $\tilde{\epsilon}-$close to their equilibrium payoff. We note that our solution is better when the set cover is smaller. Similarly, the optimality gap is tighter and $\tilde{\epsilon}$ is smaller when the set packing is bigger.

2.5 Computational Results

In this section, we demonstrate the modeling and computational advantages of our approach for the positioning of detectors in pipeline networks facing strategic attacks. First, we instantiate our detection model on a small-sized network, and illustrate how our theoretical results can be applied to achieve guaranteed detection performance against two practically relevant attack scenarios. Then, we evaluate the scalability and performance of our solution approach for a batch of large-scale networks in the water sector. All network simulations were implemented in Matlab, and all optimization problems were solved using the Gurobi solver on a computer with a 2.81 GHz Intel Core i7 processor and 16 GB of RAM.

2.5.1 Monitoring of Pipe Break and Contaminant Intrusion Events

We first consider the Apulian benchmark water network, which consists of 23 nodes and 34 pipes [39]; its layout is shown in Figure 2-7. To illustrate our approach, we consider two attack scenarios for this network: *(a)* pipeline break events, and *(b)* water contaminant intrusion events. To detect the failure events of interest, we consider that the defender has access to the relevant detection technology that is typically deployed on valve access points or fire hydrants [5, 22, 108]. For scenario *(a)*, flow and pressure sensors can indicate a potential leak or pipe break by measuring signals which can be used to detect the sudden rate of change of pressure or mass flow at different locations of the network. For scenario *(b)*, contaminant detection sensors can be used to measure water quality indicators such as electrical conductivity, free and total chlorine, turbidity, and oxygen reduction potential in the water [4].

For any given attack scenario, the set of detector locations $\mathcal{V}$ is given by the set of network nodes. Following standard modeling practice, we consider that for scenario *(a)*, the set $\mathcal{E}$ that the defender is interested in monitoring is the set of pipes; and for scenario *(b)*, this set is the set of pipes and nodes of the network. Then, for each possible detector location $i \in \mathcal{V}$, we compute the monitoring set $\mathcal{C}_i$

(defined in Section 2.2.1) which corresponds to the set of components that can be monitored from location i, depending on the type of failure events. Specifically, for scenario *(a)*, monitoring sets are computed through simulations using a threshold-based detection model, as proposed by Deshpande et al. [28] and Sela Perelman et al. [97]. In this model, a pipe break event can be detected if the distance traveled over pipes from an inspected node is less than the expected detection threshold of the propagating disturbance signal, which is typically $\sim 1\ km$ in urban water networks [107]. For scenario *(b)*, monitoring sets are constructed through simulations using a hydraulic network solver [105] that tracks the advection and reaction dynamics from a contaminant intrusion event [85, 87]. Figure 2-7 illustrates the region of a network from where the signal resulting from a pipe break (left) and a contaminant intrusion (right) can be detected. Note that in both scenarios, the network topology plays a key role in the propagation of the signal resulting from a failure event. In particular, the signal generated from a break event propagates in all directions of the network, whereas the signal from a contaminant intrusion heavily depends on the direction of the flow.

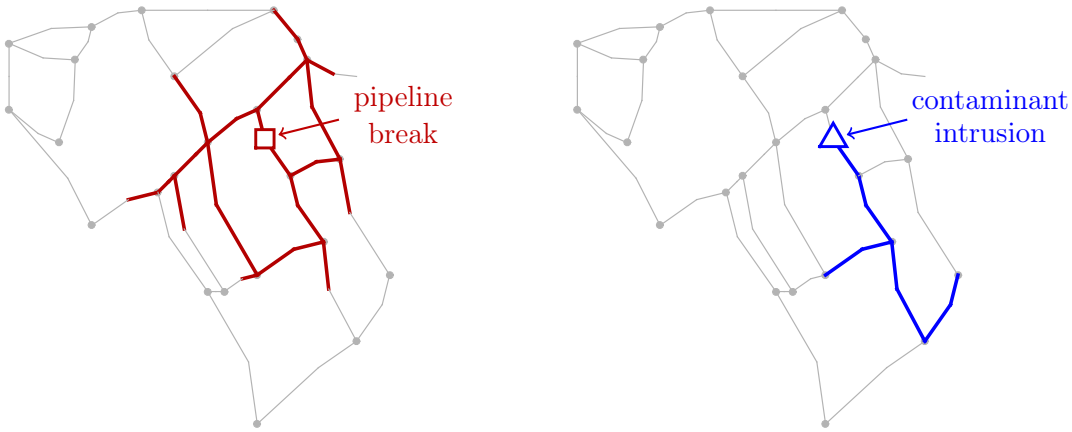
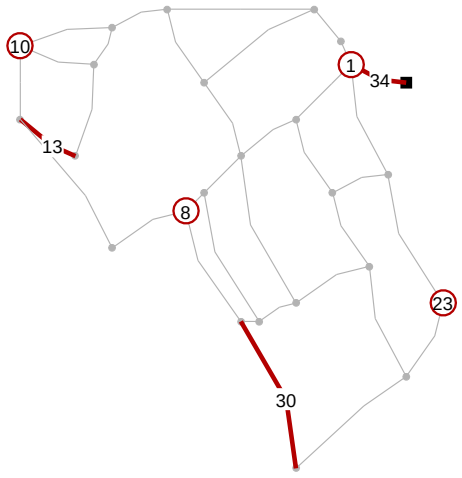


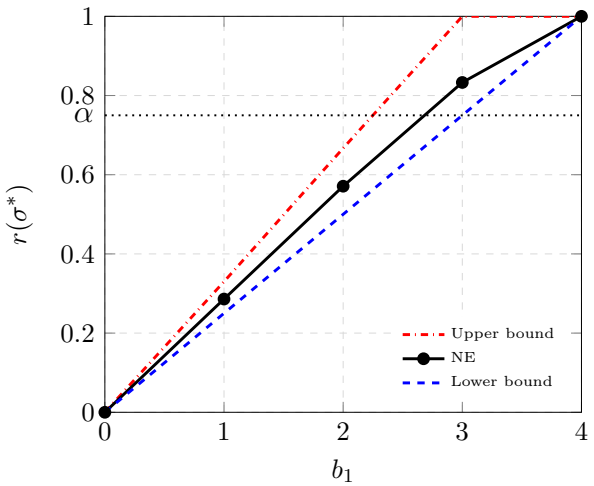
Figure 2-7: Detection model for the Apulian water network in scenario *(a)* (left) and in scenario *(b)* (right). The colored regions indicate the set of network locations from where the signal generated by the failure events can be detected.

Now, we consider the problem $(\mathcal{P})$ for scenario *(a)*, where the defender faces an adversary with $b_2 = 2$ number of attack resources (i.e., up to two pipes can be

targeted), and wants to ensure an expected detection rate of $\alpha = 0.75$. We apply our solution approach to obtain an approximate solution of $(\mathcal{P})$. Firstly, using the monitoring sets $\mathcal{C}_i$, $i \in \mathcal{V}$, we solve $(\mathcal{I}_{\text{MSC}})$ to compute an MSC $S^{min} \in \mathcal{S}$. The results show that the size of S^{min} is $n^* = 4$ (see Figure 2-8a). Then, from Theorem 1, we deduce that with $b'_1 = \lceil \alpha n^* \rceil = 3$ detectors, the expected detection rate in any equilibrium is at least α. Secondly, we solve $(\mathcal{I}_{\text{MSP}})$ to compute an MSP $T^{max} \in \mathcal{M}$, which is of size $m^* = 3$ (see Figure 2-8a). Then, from Proposition 6, we obtain that the optimality gap associated with b'_1 is given by $\lceil \alpha n^* \rceil - \lceil \alpha m^* \rceil = \lceil 3 \rceil - \lceil 2.25 \rceil = 0$. Therefore, the optimal number of detectors is $b_1^\dagger = 3$. Thirdly, given $b'_1 = 3$ and $b_2 = 2$, we use S^{min} and T^{max} to construct the strategy profile $(\sigma^1(S^{min}, b'_1), \sigma^2(T^{max}, b_2))$ according to Lemma 1. From Theorem 2, this strategy profile is an $\epsilon-$NE, and provides each player a payoff that is $\epsilon-$close to their equilibrium payoff, with $\epsilon = b'_1 b_2 \left(\frac{1}{\max\{b'_1, m^*\}} - \frac{1}{n^*} \right) = \frac{1}{2}$. Finally, Theorem 2 also gives an upper bound on the relative loss of performance by choosing $\sigma^1(S^{min}, b'_1)$ as inspection strategy, relative to an equilibrium strategy. This upper bound is given by $1 - \frac{\max\{b'_1, m^*\}}{n^*} = 25\,\%$. In fact, for this small network, we can optimally solve $(\mathcal{P})$ using (LP_1) and (LP_2) to validate the optimality guarantees provided by our solution approach; see Figure 2-8b.



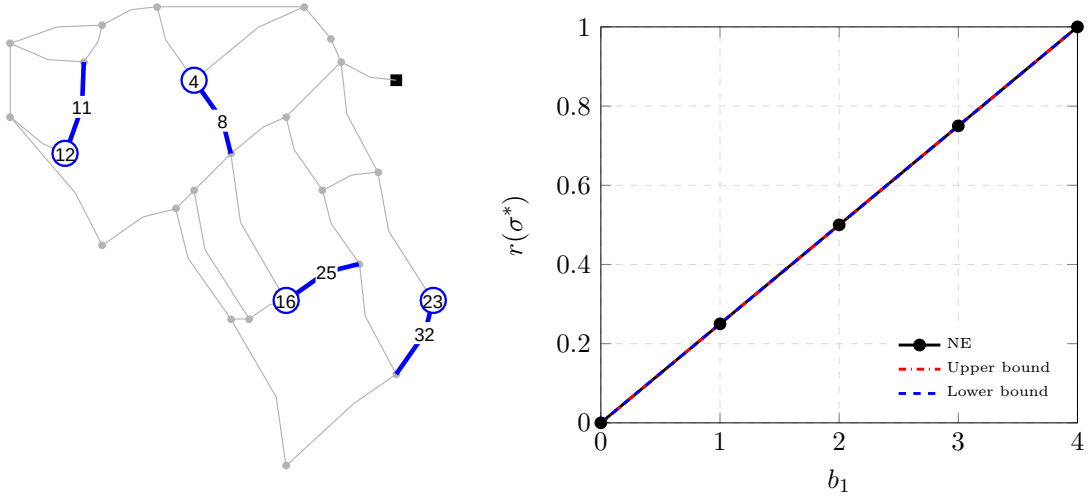
(a) MSC S^{min} (labeled nodes) and MSP T^{max} (labeled pipes).



(b) Equilibrium detection rate with respect to the number of detectors b_1.

Figure 2-8: Solving $(\mathcal{P})$ for the Apulian benchmark network facing adversarial pipeline break events.

We now consider the problem $(\mathcal{P})$ using the monitoring sets computed for the contaminant intrusion scenario *(b)* on the benchmark network. In this scenario, we notice that the optimal solutions S^{min} of $(\mathcal{I}_{\text{MSC}})$ and T^{max} of $(\mathcal{I}_{\text{MSP}})$ satisfy $|S^{min}| = n^* = m^* = |T^{max}| = 4$; see Figure 2-9. Therefore, from Proposition 6, we deduce that, for any $\alpha \in [0, 1]$ and $b_2 < m^*$, $\lceil \alpha n^* \rceil$, $(\sigma^1(S^{min}, \lceil \alpha n^* \rceil), \sigma^2(T^{max}, b_2))$ is an optimal solution of the network inspection problem $(\mathcal{P})$. In particular, for this scenario, our solution approach provides the optimal number of detectors, and their positioning in equilibrium.



(a) MSC S^{min} (labeled nodes) and MSP T^{max} (labeled pipes).

(b) Equilibrium detection rate with respect to the number of detectors b_1.

Figure 2-9: Solving $(\mathcal{P})$ for the Apulian benchmark network facing adversarial contaminant intrusion events.

2.5.2 Evaluation on Real Networks

We now test the scalability and performance of our solution approach for large-scale networks. For the sake of illustration, we consider a batch of benchmark distribution networks from the water sector that are used by researchers to test network monitoring algorithms. Table 2.4 lists the characteristics (i.e., total pipe length, and number of nodes and pipes) of the 13 networks considered in our study. The data for these networks can be found in [54, 88, 104].

For these networks, consider the scenario *(a)* introduced in Section 2.5.1, where the defender is tasked with detecting multiple pipeline leaks caused by the attacker. For each network, we apply our solution approach to construct our (approximate) solution of $(\mathcal{P})$: we first compute the monitoring sets $\mathcal{C}_i,\ i \in \mathcal{V}$. Then, we solve $(\mathcal{I}_{\text{MSC}})$ to compute the number of detectors that are sufficient to achieve the target detection performance, and to construct an inspection strategy. Next, we solve $(\mathcal{I}_{\text{MSP}})$, which enables us to evaluate the performance of our solution, i.e., we compute the optimality gap given in Proposition 6 and the relative loss of performance derived from Theorem 2. The computational results are summarized in Table 2.4.

Table 2.4: Network data and computational results, $\alpha = 0.75$.

Network	**Total length** $[km]$	**No. of pipes**	**No. of nodes**	**Running time** $[s]$ $(\mathcal{I}_{\text{MSP}})$	$(\mathcal{I}_{\text{MSC}})$	$\mathbf{m}^*$	$\mathbf{n}^*$	$\lceil \alpha \mathbf{n}^* \rceil$	**Optimality gap**	**Relative loss of performance**
bwsn1	37.56	168	126	0.05	0.11	7	7	6	0 %	0 %
ky3	91.29	366	269	0.01	0.03	15	15	12	0 %	0 %
ky5	96.58	496	420	0.02	0.05	18	19	15	1 (7.14 %)	5.3 %
ky7	137.05	603	481	0.09	0.08	28	28	21	0 %	0 %
ky6	123.20	644	543	0.08	0.06	24	24	18	0 %	0 %
ky1	166.60	907	791	0.03	0.08	31	31	24	0 %	0 %
ky13	153.30	940	778	0.06	0.08	28	30	23	2 (9.52 %)	6.7 %
ky2	152.25	1124	811	0.39	0.41	18	19	15	1 (7.14 %)	5.3 %
ky4	260.24	1156	959	0.03	0.05	62	64	48	1 (2.13 %)	3.1 %
ky8	247.34	1614	1325	0.14	0.22	45	45	34	0 %	0 %
dover	779.86	16000	14965	4.34	8.36	119	121	91	1 (1.11 %)	1.7 %
bswn2	1,844.04	14822	12523	0.77	4.06	352	361	271	7 (2.65 %)	2.5 %
mnsr	476.67	25484	24681	58.89	68.67	50	52	39	1 (2.63 %)	3.8 %

We note that the sizes of MSCs and MSPs are equal for 6 out of the 13 networks. Thus, for these 6 networks, our approach gives an optimal solution of $(\mathcal{P})$. For the remaining 7 networks, we note that the relative difference between n^* and m^* is still small, which implies that our estimate of the optimal value of $(\mathcal{P})$, $b_1' = \lceil \alpha n^* \rceil$, is close to the optimal value $b_1^\dagger$. Indeed, for these networks, when $\alpha = 0.75$, our solution is not off by more than 1 or 2 sensors, except for bswn2 for which the optimality gap is 7 sensors (which corresponds to 2.65 % of the optimal value $b_1^\dagger$ for this large network). Additionally, we can see from Table 2.4 that the relative loss of performance by

choosing $\sigma^1(S^{min}, b_1')$ in comparison to the performance in equilibrium is small (2.7 % on average over all networks). Indeed, even for the networks for which $n^* > m^*$, we obtain a relative loss of performance between 1.7 % and 6.7 %.

Finally, the time to solve the integer programming formulations (2.13)-(2.14) of ($\mathcal{I}_{\text{MSC}}$) and ($\mathcal{I}_{\text{MSP}}$) is fairly small. For networks with less than 1500 nodes and components, Gurobi computes an optimal solution in less than half a second, which directly enables us to construct an (approximate) NE. Recall that even for such medium-sized networks, (LP_1) and (LP_2) cannot be used to compute equilibrium strategies. Besides, for larger networks, we can obtain an MSC and an MSP in approximately one minute. Thus, our approach is scalable to large-scale networks, thanks to modern optimization solvers.

2.6 Additional Applications

In this section, we demonstrate the applicability of our model and results to additional settings. In particular, we show how our MSC/MSP-based strategy profile can be constructed in particular cases where the set of detector locations $\mathcal{V}$ or the set of critical network components $\mathcal{E}$ is of exponential size. We illustrate our results on a network path interdiction problem, and on a network inspection problem using small Unmanned Aircraft Systems.

2.6.1 Strategic Network Path Interdiction

Consider the setting where a security agency is concerned with dispatching up to b_1 interdictors to prevent the traffic of illegal goods through a transportation network. We model this network as a connected graph $\mathcal{H} = (\mathcal{N}, \mathcal{A})$, where $\mathcal{N}$ (resp. $\mathcal{A}$) represents the set of nodes (resp. set of edges) of the network. This network is utilized by a malicious entity composed of b_2 routers to carry illegal goods from a set of source nodes $\mathcal{N}_S \subset \mathcal{N}$ to a set of destination nodes $\mathcal{N}_T \subset \mathcal{N}$, with $\mathcal{N}_S \cap \mathcal{N}_T = \emptyset$. Each router travels along a path in $\mathcal{H}$ that originates from a node in $\mathcal{N}_S$ and terminates at a node in $\mathcal{N}_T$. We denote the set of such paths as Λ. Simultaneously, the agency

chooses up to b_1 edges to interdict.

If a router travels along a path that intersects with an edge that is inspected by an interdictor, the router is then intercepted. In this model, we suppose that the security agency wants to maximize the number of routers it intercepts, and the malicious entity wants to maximize the number of routers that successfully cross the network. Both the security agency and the malicious entity can choose a randomized strategy. Then, this problem can be modeled with our game $\Gamma(b_1, b_2)$: **P1** is the security agency, **P2** is the malicious entity, the set of "detector" locations is given by $\mathcal{V} = \mathcal{A}$ (i.e., the set of network edges), and the set of critical components of the network is $\mathcal{E} = \Lambda$ (i.e., the set of network paths that originate from $\mathcal{N}_S$ and terminate at $\mathcal{N}_T$). Furthermore, for any edge $e \in \mathcal{A}$ that is inspected, the set of paths that are monitored is given by $\mathcal{C}_e = \{\lambda \in \Lambda \mid e \in \lambda\}$.

Therefore, our MSC/MSP-based strategy profile can be computed by solving $(\mathcal{I}_{\text{MSC}})$ and $(\mathcal{I}_{\text{MSP}})$. However, in this setting, the number of constraints (resp. number of variables) in the integer programming formulation of $(\mathcal{I}_{\text{MSC}})$ (resp. $(\mathcal{I}_{\text{MSP}})$) is equal to the number of network paths in Λ, which may be exponential. Thus, (2.13) and (2.14) cannot be used to compute an MSC and an MSP.

Instead, we note that $(\mathcal{I}_{\text{MSC}})$ consists of finding a set of edges of $\mathcal{H}$ of minimum size that intersects with every path in the network. Thus, an MSC is a minimum cardinality cut-set of $\mathcal{H}$. Similarly, $(\mathcal{I}_{\text{MSP}})$ consists of finding a maximum set of edge-disjoint paths in $\mathcal{H}$. This implies that an MSP can be obtained from the path decomposition of an integral maximum flow f^* in $\mathcal{H}$ (where each edge capacity is 1).

From the max-flow min-cut theorem, we know that a minimum cardinality cut-set S^{min} and a maximum set of edge-disjoint paths T^{max} are of same size. Therefore, $n^* = m^*$. From Proposition 4, we deduce that for any $b_1 < n^*$ and $b_2 < m^*$, the strategy profile $(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2))$ defined in Lemma 1 is a NE of the game $\Gamma(b_1, b_2)$. In this equilibrium, the security agency interdicts each edge of the minimum cardinality cut-set S^{min} with probability $\frac{b_1}{n^*}$. Similarly, the malicious entity's strategy is such that each path of T^{max} is taken with probability $\frac{b_2}{m^*}$.

2.6.2 Strategic Network Inspection Using Unmanned Aircraft Systems

We now consider the inspection problem faced by an operator who is interested in monitoring an infrastructure system using a fleet of small Unmanned Aircraft Systems (sUAS). The main objective is to inspect a set of locations in order to detect component failures caused by a strategic attacker. We assume that the operator has a set of b_1 homogeneous fuel-constrained sUAS at her disposal that she can simultaneously dispatch to inspect the network. Each sUAS can be launched from a base node 0 and can visit a set of tasked locations $\mathcal{N}$ before returning to the base node. Each such exploration provides diagnostic information to the operator (i.e., presence of a component failure), and can help improve the operator's response to failures.

For every pair of locations $(i, j) \in \mathcal{N}^2$, let d_{ij} denote the amount of fuel needed by an sUAS to travel from i to j. When assigning the parameters d_{ij}, we can take into account several factors: for example, air space restrictions and obstacles can influence the shortest distance from one location to another, the height difference between two locations can influence the amount of fuel that is burnt, etc. Note that we do not impose symmetry, i.e., we allow $d_{ij} \neq d_{ji}$. This allows us to consider explorations in which sUAS take different paths during onward and return journeys between the base node and a set of target locations. We assume that the parameters d_{ij}, $(i, j) \in \mathcal{N}^2$, satisfy the triangular inequality.

We consider that all b_1 sUAS are homogeneous, i.e., they have identical sensing capabilities, and each has a fuel carrying capacity of D_{max}. For the special case when the amount of fuel required to travel from one location to another depends linearly on the traveled distance, d_{ij} can be viewed as the distance of the shortest path from i to j, and D_{max} as the maximum distance that can be traveled by each sUAS in each exploration. We will use this interpretation of d_{ij} and D_{max} from now on.

To represent the set of *feasible flight plans* of an sUAS, consider the complete directed graph $\mathcal{K} = (\mathcal{N}, \mathcal{A})$, whose set of nodes is the set of locations $\mathcal{N}$, and whose set of directed edges is $\mathcal{A} \coloneqq \{(i, j) \in \mathcal{N}^2 \mid i \neq j\}$. For each edge $(i, j) \in \mathcal{A}$, we assign

the distance from node i to j, d_{ij}, as its length. In $\mathcal{K}$, a *walk* can be represented as a sequence of $m \in \mathbb{N}$ nodes $(i_1, \ldots, i_m) \in \mathcal{N}^m$, and its length is obtained by summing up the lengths of the edges on the walk. A walk that starts and ends at the base node 0, referred to as a *0-closed walk*, can be represented as a sequence of vertices $w \coloneqq (i_1, \ldots, i_m) \in \mathcal{N}^m$ such that $i_1 = i_m = 0$. Thus, the set of feasible flight plans of an sUAS can be represented as the set of 0-closed walks of length at most D_{max} in $\mathcal{K}$, and is written as follows:

$$\mathcal{F} \coloneqq \{(i_1, \ldots, i_m) \in \mathcal{N}^m \mid i_1 = i_m = 0 \text{ and } \sum_{k=1}^{m-1} d_{i_k i_{k+1}} \leq D_{max},\ m \in \mathbb{N}\}.$$

Note that 0-closed walks allow the sUAS to visit a node more than once. Without loss of generality, we assume that every location in $\mathcal{N}$ is part of at least one feasible flight plan.

Next, we consider that the attacker can simultaneously target up to $b_2 \in \mathbb{N}$ infrastructure components. Let $\mathcal{E}$ be the set of infrastructure components that can be targeted by the strategic attacker. We assume that each location from $\mathcal{N}$ provides a vantage point to monitor nearby infrastructure components. In particular, for each location $i \in \mathcal{N}$, we consider a discrete set $\mathcal{C}_i \in 2^{\mathcal{E}}$ that represents the subset of components that an sUAS is capable of monitoring when positioned in location i. If an sUAS visits location $i \in \mathcal{N}$ and the attacker targets a component $e \in \mathcal{C}_i$, then the sUAS detects the resulting failure. In practice, the sets $\mathcal{C}_i$, $i \in \mathcal{N}$, are defined depending on the sensing capabilities of the sUAS and the environment they are operated in. For example, in the context of a wildfire monitoring application, an sUAS can use thermal/IR cameras to detect fires occurring within a certain range; in such cases, $\mathcal{C}_i$ would consist of the region around a vantage point i within that range.

In this model, we suppose that the operator wants to maximize the number of failures that she detects, while the attacker wants to maximize the number of failures that remain undetected. Furthermore, we allow the operator and the attacker to randomize over their sets of actions. Then, this problem can be modeled using our game $\Gamma(b_1, b_2)$: **P1** is the operator, **P2** is the attacker, and the set of vulnerable

components is $\mathcal{E}$. Interestingly, the set of detector "locations" $\mathcal{V}$ now represents the set of feasible flight plans $\mathcal{F}$. Furthermore, for each feasible flight plan $w \in \mathcal{F}$, the corresponding monitoring set is given by $\mathcal{C}_w = \cup_{i \in w} \mathcal{C}_i$.

Therefore, our MSC/MSP-based approximate NE can be derived for this game. However, as in Section 2.6.1, the integer programming formulation (2.13) (resp. (2.14)) of ($\mathcal{I}_{\text{MSC}}$) (resp. ($\mathcal{I}_{\text{MSP}}$)) cannot be solved for this model because of its exponential number of variables (resp. constraints). Instead, we derive two compact mixed integer programming formulations of ($\mathcal{I}_{\text{MSC}}$) and ($\mathcal{I}_{\text{MSP}}$) by exploiting the features of the model.

First, from the triangular inequality satisfied by d_{ij}, $(i,j) \in \mathcal{N}^2$, we deduce that the optimal value of ($\mathcal{I}_{\text{MSC}}$) remains unchanged when restricting its feasible solutions (i.e. sets of feasible flight plans) to be pairwise node-disjoint cycles. Therefore, we only consider feasible solutions of ($\mathcal{I}_{\text{MSC}}$) such that every location in $\mathcal{N} \backslash \{0\}$ is visited at most once. We can now provide a mixed integer programming formulation that optimally solves ($\mathcal{I}_{\text{MSC}}$). For the sake of convenience, we introduce the following notation: for every component $e \in \mathcal{E}$, let $\mathcal{N}(e) \in 2^{\mathcal{N}}$ denote the set of locations from where an sUAS can monitor e, i.e.:

$$\forall e \in \mathcal{E},\ \mathcal{N}(e) = \{i \in \mathcal{N} \mid e \in \mathcal{C}_i\}.$$

For each directed edge $(i,j) \in \mathcal{A}$ in $\mathcal{K}$, we define the binary variable x_{ij} equal to 1 if an sUAS goes from i to j, and 0 otherwise, and we define the real variable z_{ij} which is the total distance traveled by the sUAS when it reaches location j (within its cycle). Finally, let n denote the decision variable that represents the number of sUAS that are needed. ($\mathcal{I}_{\text{MSC}}$) can then be solved with the following mixed integer

program, which we denote (MSC_{UAS}):

$$
\begin{aligned}
\text{minimize} \quad & n \\
\text{subject to} \quad & \sum_{i \in \mathcal{N}(e)} \sum_{j \in \mathcal{N} \setminus \{i\}} x_{ji} \geq 1, && \forall e \in \mathcal{E} && (2.22) \\
& \sum_{j \in \mathcal{N} \setminus \{i\}} x_{ji} = \sum_{j \in \mathcal{N} \setminus \{i\}} x_{ij}, && \forall i \in \mathcal{N} && (2.23) \\
& \sum_{j \in \mathcal{N} \setminus \{0\}} x_{0j} = n && && (2.24) \\
& \sum_{j \in \mathcal{N} \setminus \{i\}} x_{ji} \leq 1, && \forall i \in \mathcal{N} \setminus \{0\} && (2.25) \\
& \sum_{j \in \mathcal{N} \setminus \{i\}} z_{ij} = \sum_{j \in \mathcal{N} \setminus \{i\}} z_{ji} + \sum_{j \in \mathcal{N} \setminus \{i\}} d_{ij} x_{ij}, && \forall i \in \mathcal{N} \setminus \{0\} && (2.26) \\
& 0 \leq z_{ij} \leq D_{max} x_{ij}, && \forall (i,j) \in \mathcal{A} && (2.27) \\
& z_{0i} = d_{0i} x_{0i}, && \forall i \in \mathcal{N} \setminus \{0\} && (2.28) \\
& x_{ij} \in \{0,1\}, && \forall (i,j) \in \mathcal{A}.
\end{aligned}
$$

Constraint (2.22) ensures that for every network component $e \in \mathcal{E}$, at least one location $i \in \mathcal{N}(e)$ that can monitor e is visited by an sUAS: Constraints (2.23)-(2.25) impose that n sUAS travel only along pairwise node-disjoint cycles: constraint (2.23) is a flow constraint (if an sUAS arrives at node i, it also needs to leave node i); constraint (2.24) forces that all the n sUAS leave the launching site, and (2.25) does not allow a node (except 0) to be visited more than once.

Constraints (2.26)-(2.28) model the limit on the maximum distance traveled by each sUAS. Constraint (2.26) computes the distance traveled so far by an sUAS when flying over each location. Notice that this constraint, first introduced by Kara [55] and Waters [113], also ensures the elimination of subtours that usually arise in these types of problems (analogous to the MTZ formulation of the Traveling Salesman Problem [76]). Constraint (2.27) enforces the distance traveled by each sUAS to be at most D_{max}, and sets z_{ij} to be equal to 0 if edge (i,j) is not taken by any sUAS. Finally, constraint (2.28) initializes the total distance traveled by an sUAS when it leaves the

base node.

We note that we do not require the sUAS to visit all the locations in $\mathcal{N}$, as long as all the network components are monitored. In the specific case where each location needs to be visited by at least one sUAS, then we find again the classical *distance-constrained vehicle routing problem* (with minimization of the number of vehicles) widely studied in the literature [3, 56, 66, 67, 77, 99]. This entails that (MSC_{UAS}) is an NP-hard problem.

Secondly, we note that in this model, ($\mathcal{I}_{\text{MSP}}$) consists of finding a maximum set of components $T^{max} \subseteq \mathcal{E}$ such that there is no feasible flight plan that can monitor more than one component in T^{max}. More specifically, for any two components $e_1 \neq e_2 \in T^{max}$, there is no feasible flight plan that can visit a location $i_1 \in \mathcal{N}(e_1)$ and a location $i_2 \in \mathcal{N}(e_2)$. If for every pair of locations $(i,j) \in \mathcal{N}^2$, there exists a feasible flight plan that visits location i and j, then MSPs are of size 1. Henceforth, we assume that there exists a pair of locations $(i,j) \in \mathcal{N}^2$ that cannot be visited as part of a feasible flight plan.

Importantly, a 0-closed walk of shortest length that visits any two locations $i_1 \neq i_2 \in \mathcal{N}$ has a length equal to $\min\{d_{0i_1} + d_{i_1i_2} + d_{i_20}, d_{0i_2} + d_{i_2i_1} + d_{i_10}\}$. We can now derive an integer programming formulation that optimally solves ($\mathcal{I}_{\text{MSP}}$). For each component e $\in \mathcal{E}$, we define the binary variable y_e equal to 1 if e is part of the MSP, and 0 otherwise. We denote (MSP_{UAS}) the following optimization problem:

$$\text{maximize} \quad \sum_{e \in \mathcal{E}} y_e \tag{2.29}$$

$$\text{subject to} \quad d_{0i} + d_{ij} + d_{j0} \geq (D_{max} + \epsilon)\Big(\sum_{e \in \mathcal{C}_i \cup \mathcal{C}_j} y_e - 1\Big), \qquad \forall (i,j) \in \mathcal{N}^2 \tag{2.30}$$

$$y_e \in \{0,1\}, \qquad \forall e \in \mathcal{E},$$

where $\epsilon = \min\{d_{0i} + d_{ij} + d_{j0} - D_{max} \mid d_{0i} + d_{ij} + d_{j0} > D_{max}, (i,j) \in \mathcal{N}^2\}$. Objective (2.29) maximizes the number of components to include in the set packing. Interestingly, our formulation only requires constraints (2.30). First, note that (MSP_{UAS}) is feasible: $y_e = 0$, for every $e \in \mathcal{E}$ is a feasible solution. Now, let y be a fea-

sible solution of (MSP_{UAS}), and consider a feasible flight plan $(0, i, j, 0) \in \mathcal{F}$ visiting locations i and j. Since $d_{0i} + d_{ij} + d_{j0} \leq D_{max}$, then necessarily $(\sum_{e \in \mathcal{C}_i \cup \mathcal{C}_j} y_e - 1) \leq 0$ (otherwise, we would have $D_{max} + \epsilon \leq D_{max}$). From the triangular inequality, we conclude that any feasible flight plan only monitors one element e such that $y_e = 1$: the support of y is a set packing.

Now, consider a set packing $T \subseteq \mathcal{E}$, and let y be such that $y_e = \mathbb{1}_{\{e \in T\}}$. By definition of a set packing, we deduce that for any feasible flight plan $(0, i, j, 0) \in \mathcal{F}$, $\sum_{e \in \mathcal{C}_i \cup \mathcal{C}_j} y_e \leq 1$. Therefore, constraints (2.30) are satisfied for $(i, j) \in \mathcal{N}^2$ such that $(0, i, j, 0) \in \mathcal{F}$. Now, consider $(i, j) \in \mathcal{N}^2$ such that $(0, i, j, 0) \notin \mathcal{F}$. Then, necessarily, $d_{0i} + d_{ij} + d_{j0} \geq D_{max} + \epsilon$. Furthermore, since i is part of at least one feasible flight plan (i.e., $(0, i, 0) \in \mathcal{F}$), and by definition of T, we deduce that $\sum_{e \in \mathcal{C}_i} y_e \leq 1$. Similarly, we obtain that $\sum_{e \in \mathcal{C}_j} y_e \leq 1$. Therefore:

$$\sum_{e \in \mathcal{C}_i \cup \mathcal{C}_j} y_e \leq \sum_{e \in \mathcal{C}_i} y_e + \sum_{e' \in \mathcal{C}_j} y_{e'} \leq 2,$$

which implies that:

$$(D_{max} + \epsilon)\big(\sum_{e \in \mathcal{C}_i \cup \mathcal{C}_j} y_e - 1\big) \leq (D_{max} + \epsilon) \leq d_{0i} + d_{ij} + d_{j0}.$$

Therefore, y is a feasible solution of (MSP_{UAS}). We can then conclude that (MSP_{UAS}) is an integer programming formulation of ($\mathcal{I}_{\text{MSP}}$).

Example 5. Next, we illustrate our results with three example networks.

Star Network: Consider the network in Figure 2-10.

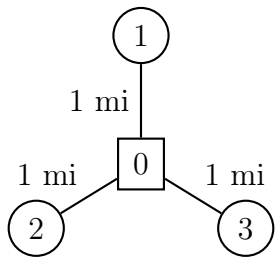
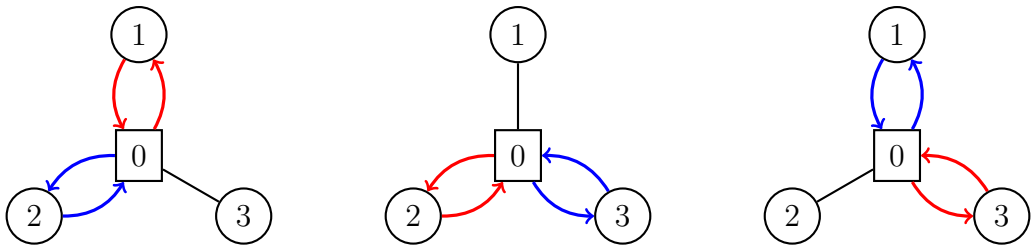


Figure 2-10: A star network.

This example has the base node 0 and three other locations $\{1, 2, 3\}$ that are at a distance of 1 mile from the base node. There are three infrastructure components e_1, e_2, and e_3 that can be respectively monitored from locations 1, 2, and 3. Finally, assume that the sUAS can travel for 2 miles.

Then, the optimal value of $(\mathcal{I}_{\text{MSC}})$ is $n^* = 3$, and the optimal solution is $S^{min} = \{(0, 1, 0), (0, 2, 0), (0, 3, 0)\}$.

Now, suppose that the operator has two sUAS. Then, the dispatches in the support of $\sigma^1(S^{min}, 2)$ are $S^1 = \{(0, 1, 0), (0, 2, 0)\}$, $S^2 = \{(0, 2, 0), (0, 3, 0)\}$, and $S^3 = \{(0, 3, 0), (0, 1, 0)\}$, and are each chosen with probability $\frac{1}{3}$. Since each of these 0-closed walks is in exactly 2 dispatches in the support of $\sigma^1(S^{min}, 2)$, then each one of them is taken with probability $\frac{2}{3} = \frac{b_1}{n^*}$. $\sigma^1(S^{min}, 2)$ is shown in Figure 2-11.



(a) $\sigma^1(S^{min}, 2)_{S^1} = \frac{1}{3}$. (b) $\sigma^1(S^{min}, 2)_{S^2} = \frac{1}{3}$. (c) $\sigma^1(S^{min}, 2)_{S^3} = \frac{1}{3}$.

Figure 2-11: Randomized dispatch on the star network.

Furthermore, no sUAS can monitor two components with a single feasible flight plan. This implies that the MSP is $T^{max} = \{e_1, e_2, e_3\}$. Therefore, for any number of attack resources $b_2 < m^* = 3$, the attacker's strategy $\sigma^2(T^{max}, b_2)$ is such that each component in T^{max} is targeted with probability $\frac{b_2}{m^*}$. From Proposition 4, we deduce that $(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2))$ is a NE of the game $\Gamma(b_1, b_2)$, for any $b_1 < 3$ and $b_2 < 3$.

Complete Network: Consider the fully connected network given in Figure 2-12 consisting of 10 locations uniformly placed on a circle of radius 1 mile. The distance between each pair of node is the Euclidean distance. The sUAS can fly for 4 miles. The set of vulnerable components is only comprised of the network edges, and an sUAS at location i can only monitor the edges adjacent to i.

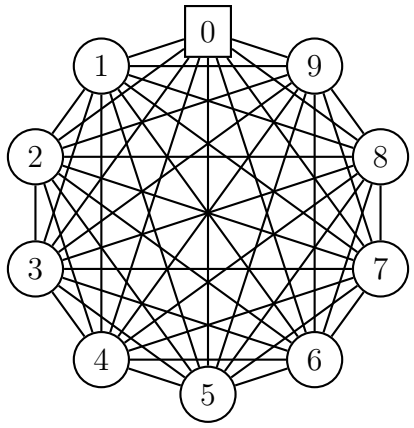
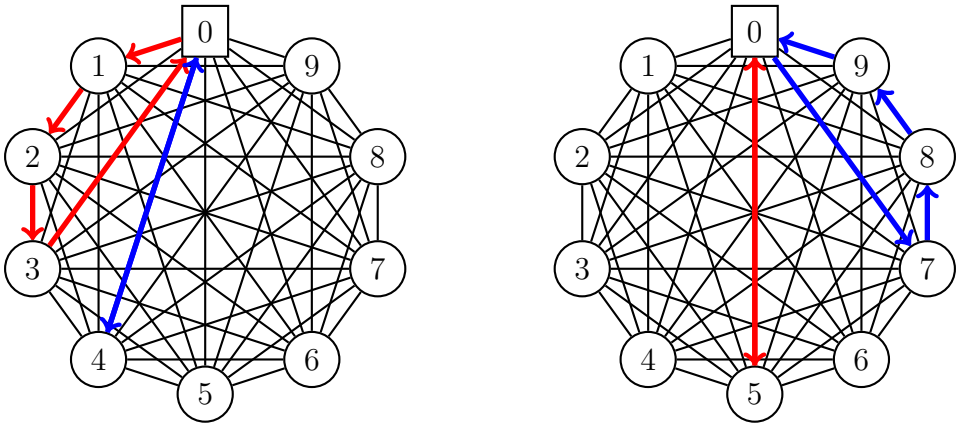


Figure 2-12: A complete network.

After solving (MSC_{UAS}), we obtain that the minimum number of sUAS needed to monitor all the edges of the network is $n^* = 4$, and they can respectively be sent along the cycles $w_1^* = (0, 1, 2, 3, 0)$, $w_2^* = (0, 4, 0)$, $w_3^* = (0, 5, 0)$ and $w_4^* = (0, 7, 8, 9, 0)$. Note that all but one locations are visited by an sUAS. Now, if the operator only has 2 sUAS, she can randomize their dispatch according to the following probability distribution $\widetilde{\sigma}^1$: send them along $\{w_1^*, w_2^*\}$ with probability $\frac{1}{2}$, and along $\{w_3^*, w_4^*\}$ with probability $\frac{1}{2}$; see Figure 2-13.



(a) $\widetilde{\sigma}^1_{S^1} = \dfrac{1}{2}$ (b) $\widetilde{\sigma}^1_{S^2} = \dfrac{1}{2}$

Figure 2-13: Randomized dispatch on the complete network.

Tree Network: Now, consider a binary tree network given in Figure 2-14 consisting of 15 locations, and whose edges are of length 1 mile. Assume that the sUAS can only travel along the edges of the tree, and can travel for 12 miles.

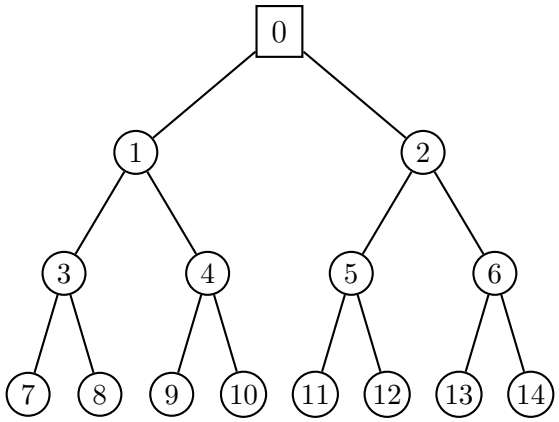
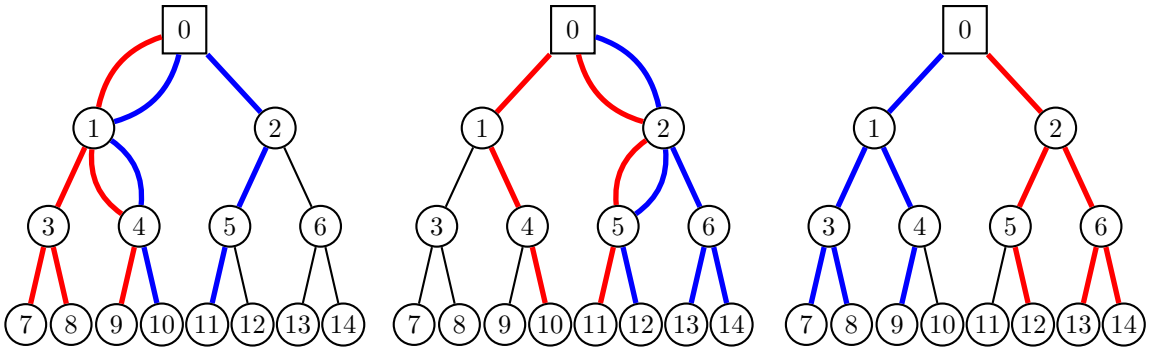


Figure 2-14: A tree network.

Thus, to compute the shortest distance between each pair of nodes d_{ij}, $(i,j) \in \mathcal{N}^2$, one can run Floyd-Warshall Algorithm [34]. We now assume that the set of vulnerable components is only comprised of nodes of the tree, and that the sUAS need to visit the node in order to monitor it. First, we solve (MSC_{UAS}): the minimum number of sUAS needed to monitor all the nodes of the network is $n^* = 3$, and they can respectively be sent along the cycles $w_1^* = (0,1,3,7,8,9,4,0)$, $w_2^* = (0,10,2,5,11)$, and $w_3^* = (0,12,6,13,14)$ in the directed graph $\mathcal{K}$. Note that even though w_1^* is a cycle in $\mathcal{K}$, the actual walk that an sUAS traveling according to w_1^* is taking (in the tree network) is $(0,1,3,7,3,8,3,1,4,9,4,1,0)$. Let $S^{min} = \{w_1^*, w_2^*, w_3^*\}$. Now, if the operator only has 2 sUAS, she can randomize their dispatch according to $\sigma^1(S^{min}, 2)$: send them along $\{w_1^*, w_2^*\}$ with probability $\frac{1}{3}$, along $\{w_2^*, w_3^*\}$ with probability $\frac{1}{3}$, and along $\{w_3^*, w_1^*\}$ with probability $\frac{1}{3}$. The strategy $\sigma^1(S^{min}, 2)$ is illustrated in Figure 2-15.

$\triangle$

Therefore, in this section, we demonstrated additional modeling advantages of our game. In particular, our detection model can be applied to settings where the set of detector locations or the set of critical network components is given by network paths. To overcome the exponential size of the integer programming formulations of ($\mathcal{I}_{\text{MSC}}$) and ($\mathcal{I}_{\text{MSP}}$) that we derived in Section 2.3.1, we exploited the structure of the problems we considered. For the strategic network path interdiction problem, we showed that



(a) $\sigma^1(S^{min}, 2)_{S^1} = \frac{1}{3}$ (b) $\sigma^1(S^{min}, 2)_{S^2} = \frac{1}{3}$ (c) $\sigma^1(S^{min}, 2)_{S^3} = \frac{1}{3}$

Figure 2-15: Randomized dispatch on the tree network.

($\mathcal{I}_{\text{MSC}}$) and ($\mathcal{I}_{\text{MSP}}$) could be solved efficiently by computing a max-flow and minimum cardinality cut-set of the transportation network. For the strategic network inspection problem using sUAS, we formulated ($\mathcal{I}_{\text{MSC}}$) as a vehicle routing problem that we solved thanks to a mixed integer programming formulation. Furthermore, we showed that ($\mathcal{I}_{\text{MSC}}$) could be formulated using a compact integer program.

2.7 Refinement Procedure for Exactly Solving ($\mathcal{P}$)

The computational results in Section 2.5 indicate that our solution approach is scalable to realistic instances of ($\mathcal{P}$) and provides reasonable performance guarantees. However, one can construct a particular example for which the guarantees provided by our solution approach are arbitrarily bad:

Example 6. Consider a graph $\mathcal{H} = (\mathcal{N}, \mathcal{A})$, where $\mathcal{N} = [\![1, n]\!]$ is the set of vertices, and $\mathcal{A} = \{(i, j) \in \mathcal{N}^2 \mid i \neq j\} \backslash \{(1, 2)\}$ is the set of edges. Let the detection model be such that $\mathcal{V} = \mathcal{A}$, $\mathcal{E} = \mathcal{N}$, and $\forall i = (u, v) \in \mathcal{V}$, $\mathcal{C}_i = \{u, v\}$. Then, in this case, an MSC is a minimum edge cover of $\mathcal{H}$, which is of size $\lceil \frac{n}{2} \rceil$, and an MSP is a maximum independent set of $\mathcal{H}$, which is only of size 2. Consider that **P2** has $b_2 = 1$ unit of resources, and the target detection rate is $\alpha \in [0, 1]$. Then, as the size of the graph n increases, the upper bound on the optimality gap of our solution given in Proposition 6 is equal to $\lceil \alpha \lceil \frac{n}{2} \rceil \rceil - \lceil 2\alpha \rceil \underset{n \to +\infty}{\longrightarrow} +\infty$. Furthermore, for $b_1 = b_2 = 1$,

the relative loss of performance of our MSC-based inspection strategy, derived from Theorem 2, is equal to $1 - \frac{2}{\lceil n/2 \rceil} \underset{n \to +\infty}{\longrightarrow} 100\,\%$. $\triangle$

More importantly, the defender might desire an inspection strategy that outperforms our MSC-based strategy by requiring less number of detectors. In this section, we develop a procedure that iteratively refines the MSC/MSP-based solution proposed in Proposition 6 to provide a stronger performance guarantee, until it reaches optimality of $(\mathcal{P})$. This procedure relies on an important and rather surprising property of the expected detection rate in equilibrium of the game Γ, which we describe next.

2.7.1 Impact of P2's Resources on Detection Performance

We recall from Section 2.3.3 that when $n^* = m^*$, the expected detection rate in equilibrium of $\Gamma(b_1, b_2)$ with $b_2 < m^*$, is equal to $\frac{b_1}{n^*}$ (Eq. (2.20)). That is, it does not depend on **P2**'s resources b_2. In fact, we can show that this property holds in general, as long as $b_2 < m^*$:

Theorem 3. *Given a detection model $\mathcal{G}$, and **P1**'s resources $b_1 \in \mathbb{N}$, the expected detection rate in equilibrium is identical in any game $\Gamma(b_1, b_2)$, with $b_2 < m^*$; we denote it as $r^*_{b_1}$.*

$$\forall b_1 \in \mathbb{N},\ \exists\, r^*_{b_1} \in [0,1] \mid \forall b_2 < m^*,\ \forall \sigma^* \in \Sigma(b_1, b_2), \quad r(\sigma^*) = r^*_{b_1}.$$

This result is trivial when $b_1 \geq n^*$, since the expected detection rate in equilibrium is 1, regardless of **P2**'s resources. So, our proof in Section 2.9.4 focuses on the case when $b_1 < n^*$ (and $b_2 < m^*$). Thanks to Proposition 2, proving Theorem 3 is equivalent to showing the following claim: for a fixed number of detectors $b_1 < n^*$, **P1**'s equilibrium payoff is linear with respect to b_2. From Proposition 2, we also know that **P2**'s strategy in equilibrium is an optimal solution of $(\overline{\mathrm{LP}_2})$ which, by additivity of F, can be rewritten as $\min_{\sigma^2 \in \Delta(\overline{\mathcal{A}_2})} \max_{S \in \overline{\mathcal{A}_1}} \sum_{e \in \mathcal{E}} \rho_{\sigma^2}(e)\, \mathrm{F}(S, e)$ where $\rho_{\sigma^2}(e)$ is the probability of component $e \in \mathcal{E}$ being targeted by **P2**. Thus, our claim

can be restated as follows: There exists an attack strategy in equilibrium of the game $\Gamma(b_1, 1)$, denoted σ^{2^*}, and there exists an attack strategy in equilibrium for any game $\Gamma(b_1, b_2)$ with $b_2 < m^*$, denoted $\sigma^{2'}$, such that the corresponding attack probabilities of each component $e \in \mathcal{E}$ satisfy $\rho_{\sigma^{2'}}(e) = b_2 \rho_{\sigma^{2^*}}(e)$. Showing this would imply that **P1**'s equilibrium payoff, given by the optimal value of $(\overline{\text{LP}_2})$, is linear with respect to b_2.

The above-mentioned claim is proven in two steps: First, we show that there exists an attack strategy in equilibrium of $\Gamma(b_1, 1)$, σ^{2^*}, such that the corresponding attack probability of each component $e \in \mathcal{E}$ satisfies $\rho_{\sigma^{2^*}}(e) \leq \frac{1}{m^*}$. The intuition is that given **P2**'s strategy, **P1**'s best response is to allocate detectors to the nodes from where she can monitor the components that are targeted by **P2** with highest probability. Therefore, in equilibrium, **P2** would allocate her attack resources in order to minimize the maximum expected number of detections from **P1**. Because of **P2**'s ability to spread her attacks in the network (captured by Proposition 1 and MSPs) and the submodularity of F, this results in at least m^* components with identical (highest) probability of being targeted. This first step implies that for any $b_2 < m^*$ and any component $e \in \mathcal{E}$, $b_2 \rho_{\sigma^{2^*}}(e) \leq 1$.

The second step then consists in proving that given $b_2 < m^*$, there exists an attack strategy in equilibrium of $\Gamma(b_1, b_2)$, $\sigma^{2'}$, for which each component $e \in \mathcal{E}$ is targeted with probability $b_2 \rho_{\sigma^{2^*}}(e)$ (which is now guaranteed to be no more than 1). The existence of such an attack strategy is shown using Farkas' lemma; moreover, the additivity of F ensures that this attack strategy is in fact optimal for $(\overline{\text{LP}_2})$. Thus, we complete proving the claim that **P1**'s equilibrium payoff is linear with respect to b_2, which directly implies that the expected detection rate does not depend on b_2 in equilibrium. Indeed, from Proposition 2, the expected detection rate in equilibrium is equal to **P1**'s equilibrium payoff divided by b_2. It is important to stress that this whole argument holds because the network is large in comparison to **P2**'s resources, i.e., $b_2 < m^*$. In fact, Theorem 3 also holds when $b_2 = m^*$, but counterexamples can be found when $b_2 > m^*$; see Section 2.8.1.

An immediate consequence of Theorem 3 and Proposition 2 is that both players'

equilibrium payoffs can be expressed as follows:

$$\forall b_1 < n^*,\ \forall b_2 < m^*,\ \forall (\sigma^{1^*}, \sigma^{2^*}) \in \Sigma(b_1, b_2),\ \begin{cases} U_1(\sigma^{1^*}, \sigma^{2^*}) = b_2\, r^*_{b_1} \\ U_2(\sigma^{1^*}, \sigma^{2^*}) = b_2\, (1 - r^*_{b_1}). \end{cases} \tag{2.31}$$

For the special case when $n^* = m^*$, $r^*_{b_1} = \frac{b_1}{n^*}$ (from (2.20)) and we find again (2.19) from (2.31). Another implication of Theorem 3 is that the optimal value of $(\mathcal{P})$ does not depend on b_2 (since the equilibrium constraints (2.9) can be replaced by $r^*_{b_1} \geq \alpha$). Finally, we derive from Theorem 3 the following result on equilibrium inspection strategies in the game Γ:

Proposition 7. *Given **P1**'s number of detectors $b_1 < n^*$, inspection strategies in equilibrium of the game $\Gamma(b_1, 1)$ are also inspection strategies in equilibrium of any game $\Gamma(b_1, b_2)$ with $b_2 < m^*$.*

Therefore, we can solve the problem $(\mathcal{P})$ by considering that $b_2 = 1$! From a computational viewpoint, this conclusion provides a significant advantage, which we discuss next.

2.7.2 Column Generation Procedure

Recall from Proposition 2 that the inspection strategies in equilibrium of the game $\Gamma(b_1, b_2)$ are the optimal solutions of the linear program $(\overline{\mathrm{LP}_1})$, which has $\binom{|\mathcal{V}|}{b_1} + 1$ variables and $\binom{|\mathcal{E}|}{b_2} + 1$ constraints. Now, given $b_1 < n^*$, and by considering that $b_2 = 1$, the optimal value of $(\overline{\mathrm{LP}_1})$ is the expected detection rate in equilibrium $r^*_{b_1}$ (see (2.31)), and its optimal solutions are inspection strategies in equilibrium of *any* game $\Gamma(b_1, b_2)$ with $b_2 < m^*$ (Proposition 7). Thus, $(\overline{\mathrm{LP}_1})$ can now be reformulated with $\binom{|\mathcal{V}|}{b_1}+1$ variables and only $|\mathcal{E}|+1$ constraints, and one can use column generation to solve it [26].

Each iteration of the column generation algorithm involves solving a master problem and a subproblem. Essentially, the master problem is a restricted version of $(\overline{\mathrm{LP}_1})$, where only a subset of variables is considered. Formally, given a subset $\mathcal{I} \subseteq \overline{\mathcal{A}_1}$ of

indices, the master problem of the column generation algorithm applied to $(\overline{\mathrm{LP}_1})$ is given by:

$$
\begin{aligned}
(P_{\mathrm{CG}}): \quad \text{maximize} \quad & z \\
\text{subject to} \quad & z \leq \sum_{S \in \mathcal{I}} \mathrm{F}(S,e)\sigma_S^1, \quad \forall e \in \mathcal{E} \\
& \sum_{S \in \mathcal{I}} \sigma_S^1 = 1 \\
& \sigma_S^1 \geq 0, \qquad\qquad \forall S \in \mathcal{I}.
\end{aligned}
$$

Let σ^{1^*}, z^* (resp. ρ_e^*, $(e \in \mathcal{E})$, z'^*) denote the optimal primal (resp. dual) solution of (P_{CG}).

Once the master problem is solved, the optimal dual variables are used to construct the subproblem, which involves finding the variable in the unrestricted $(\overline{\mathrm{LP}_1})$ with highest reduced cost. The reduced cost associated with each $S \in \overline{\mathcal{A}_1}$ is given by $\sum_{e \in \mathcal{E}} \mathrm{F}(S,e)\rho_e^* - z'^*$. Therefore, the detector positioning with the highest reduced cost can be obtained by solving a maximum weighted covering set problem, which can be formulated as the following integer program:

$$
\begin{aligned}
(D_{\mathrm{CG}}): \quad \text{maximize} \quad & \sum_{e \in \mathcal{E}} \rho_e^* y_e \\
\text{subject to} \quad & y_e \leq \sum_{\{i \in \mathcal{V} \,|\, e \in \mathcal{C}_i\}} x_i, \qquad \forall e \in \mathcal{E} \\
& \sum_{i \in \mathcal{V}} x_i = b_1 \\
& x_i, y_e \in \{0,1\}, \qquad \forall i \in \mathcal{V},\ \forall e \in \mathcal{E}.
\end{aligned}
$$

If the optimal value of (D_{CG}) is no more than z'^*, then this proves that the optimal primal solution of (P_{CG}), (σ^{1^*}, z^*), is also an optimal solution of $(\overline{\mathrm{LP}_1})$. However, if the optimal value of (D_{CG}) is more than z'^*, then we add the detector positioning corresponding to the optimal solution of (D_{CG}) to the set of indices $\mathcal{I}$. (P_{CG}) is then solved with the new set of indices $\mathcal{I}$. This process is repeated until the highest reduced cost computed from the subproblem is nonpositive, which certifies that the current optimal solution of the master problem is also optimal for the unrestricted $(\overline{\mathrm{LP}_1})$.

Note that this algorithm can be initiated by considering $\mathcal{I} = \text{supp}(\sigma^1(S^{min}, b_1))$, where $S^{min} \in \mathcal{S}$ is an MSC.

Thus, we finally arrive at the following computational procedure to *exactly* solve problem $(\mathcal{P})$:

Refinement Procedure

- Build the detection model $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \{\mathcal{C}_i,\ i \in \mathcal{V}\})$
- Compute an MSC $S^{min} \in \mathcal{S}$ and its size n^* by solving $(\mathcal{I}_{\text{MSC}})$
- Choose $\lceil \alpha n^* \rceil$ as initial value of b_1
- For each decreasing value of b_1, solve $(\overline{\text{LP}_1})$ by considering $b_2 = 1$ using the following steps:
  - Construct the MSC-based inspection strategy $\sigma^1(S^{min}, b_1)$
  - Run the column generation algorithm, using $\sigma^1(S^{min}, b_1)$ as a warm-start
  - At termination, obtain an equilibrium inspection strategy which uses b_1 detectors, and has expected detection rate $r^*_{b_1}$
- Stop the overall procedure if $r^*_{b_1} < \alpha$

Note that the above procedure is guaranteed to terminate at optimality, since we can argue that $b_1 \mapsto r^*_{b_1}$ is strictly increasing on $[\![0, n^*]\!]$. Indeed, if there exists $b_1 < n^*$ such that $r^*_{b_1} = r^*_{b_1+1}$, then an inspection strategy in equilibrium of $\Gamma(b_1, b_2)$ (which randomizes the positioning of b_1 detectors) is also an inspection strategy in equilibrium of $\Gamma(b_1 + 1, b_2)$; this contradicts Proposition 2.

After each iteration of the column generation algorithm on $(\overline{\text{LP}_1})$, let $\sigma^{1'}$ and r' respectively denote the current inspection strategy and value of the objective function; note that $r' = \min_{e \in \mathcal{E}} U_1(\sigma^{1'}, e)$. Then, one can derive performance guarantees for $\sigma^{1'}$ by solving $(\mathcal{I}_{\text{MSP}})$, similarly to Theorem 2. Indeed, given m^*, an upper bound on the relative loss of performance is given by $\ell' = 1 - \frac{\max\{b_1, m^*\}}{b_1} r'$. Furthermore, for any $b_2 < m^*$, one can use Lemma 1 to construct an MSP-based attack strategy.

The resulting strategy profile $(\sigma^{1'}, \sigma^2(T^{max}, b_2))$ is an $\epsilon'-$NE of $\Gamma(b_1, b_2)$ and provides both players payoffs that are $\epsilon'-$close to their respective equilibrium payoffs, where $\epsilon' = b_1 b_2(\frac{1}{\max\{b_1, m^*\}} - \frac{r'}{b_1})$. Note that when the MSC-based inspection strategy $\sigma^1(S^{min}, b_1)$ is used as an initial feasible solution for the column generation algorithm, the first iteration of the master problem will give $r' = \frac{b_1}{n^*}$, for which we find again the expressions of ϵ and the relative loss of performance from Theorem 2. Then, as the number of iterations of the column generation algorithm increases, r' increases, which causes ϵ' and ℓ' to decrease: thus, the inspection strategy improves with each iteration.

Furthermore, given $b'_1 \leq \lceil \alpha n^* \rceil$, we can note that if an iteration of the column generation method outputs an objective value that satisfies $r' \geq \alpha$, b'_1 becomes a feasible solution for the problem $(\mathcal{P})$; the reason is that r' is a lower bound on the optimal value of $(\overline{\text{LP}_1})$, $r^*_{b'_1}$. Similarly, MSPs can be used to derive an optimality gap associated with this new feasible solution: Since $b_1^\dagger \geq \lceil \alpha m^* \rceil$ (Proposition 6), an optimality gap is then given by $b'_1 - \lceil \alpha m^* \rceil$. Of course, for each decreasing value of b'_1, the optimality gap decreases as well.

When $(\overline{\text{LP}_1})$ is solved to optimality for a given b_1, the optimal dual variables ρ^*_e, $\forall e \in \mathcal{E}$, give the probabilities with which each component can be targeted in equilibrium of the game $\Gamma(b_1, 1)$. In the proof of Theorem 3, we show how to reallocate these probabilities to create an attack strategy in equilibrium of $\Gamma(b_1, 1)$ with the additional property that each component is not targeted with probability more than $\frac{1}{m^*}$. Then, from Lemma 8, given $b_2 < m^*$, we can obtain an attack strategy in equilibrium of $\Gamma(b_1, b_2)$, denoted $\sigma^2 \in \Delta(\overline{\mathcal{A}_2})$, by solving the following linear program:

$$\begin{aligned} \boldsymbol{A}\sigma^2 &= b_2 \rho^* \\ \sigma^2 &\geq \mathbf{0}_{|\overline{\mathcal{A}_2}|}, \end{aligned}$$

where $\boldsymbol{A} = (\mathbb{1}_{\{e \in T\}})_{(e,T) \in \mathcal{E} \times \overline{\mathcal{A}_2}}$. This can be done by considering the following auxiliary

problem:

$$\begin{aligned} \text{minimize} \quad & \mathbf{1}_{|\mathcal{E}|}^{\top} s \\ \text{subject to} \quad & \boldsymbol{A}\sigma^2 + s = b_2\rho^* \\ & \sigma^2 \geq \mathbf{0}_{|\overline{\mathcal{A}_2}|},\ s \geq \mathbf{0}_{|\mathcal{E}|}. \end{aligned}$$

This auxiliary problem can also be solved using column generation, with $(\sigma^2, s) = (\mathbf{0}_{|\overline{\mathcal{A}_2}|}, b_2\rho^*)$ as initial feasible solution. Given the current master problem generated by the column generation algorithm, let $\beta^* \in \mathbb{R}^{|\mathcal{E}|}$ denote its optimal dual variables. Then, the index T^* with lowest reduced cost is given by $T^* \in \arg\max_{T \in \overline{\mathcal{A}_2}} \sum_{e \in T} \beta_e^*$, i.e., T^* targets the components with highest values β_e^*. From Lemma 8, we know that at optimality, the objective value is 0 (i.e., $s = \mathbf{0}_{|\mathcal{E}|}$) and σ^2 is an equilibrium attack strategy. In summary, given $b_1 < n^*$ and $b_2 < m^*$, two column generation algorithms can be run in order to obtain an *exact* NE of game $\Gamma(b_1, b_2)$.

A downside of this refinement procedure is that it throws away the simplicity of our initial inspection strategy $\sigma^1(S^{min}, b_1)$. In practice, the defender may prefer inspection strategies with smaller support for ease of implementation. While our MSC-based inspection strategy $\sigma^1(S^{min}, b_1)$ uniformly randomizes over n^* detector positionings, the column generation algorithm can output in principle an equilibrium strategy with a support of size $|\mathcal{E}|$, which may be much larger than n^*. Thus, scheduling inspection operations according to this new strategy may require a larger level of effort. In contrast, our MSC-based inspection strategy is more amenable for periodic scheduling of inspections.

Additionally, recall that there are settings where network locations need to be initially prepared for the installation of detectors. In such cases, it is in the defender's best interest to minimize the number of such locations (represented in our model by the node basis). Our MSC-based inspection strategy only requires n^* locations to be prepared, and we showed that this number is optimal when $n^* = m^*$. On the contrary, the inspection strategy computed using column generation can have a node basis of size up to $b_1|\mathcal{E}|$, which may drastically increase the cost of preparing network locations to receive detectors. One possibility is to run few iterations of the column

generation algorithm, and stop when the inspection strategy achieves a desirable tradeoff between detection guarantee and support size.

2.8 Discussion

In this section, we discuss the case when **P2** has at least m^* attack resources. In particular, we show by way of an example which of our results still hold. Then, we conclude by summarizing our contributions in this chapter.

2.8.1 Case When $b_2 \geq m^*$

As argued in Section 2.3.1, the network inspection problem $(\mathcal{P})$ when $b_2 \geq m^*$ is of limited practical interest. However, for the sake of completeness, we now briefly discuss this case. First, recall from Section 2.3.1 that the optimal value of $(\mathcal{P})$ is no more than n^*, since **P1** can achieve any target detection rate when she has at least n^* detectors; thus, we will continue to restrict our attention to the game $\Gamma(b_1, b_2)$ when $b_1 < n^*$.

To evaluate the equilibrium constraints (2.9)-(2.10), we derived in Section 2.3 equilibrium properties of the game $\Gamma(b_1, b_2)$ that hold when $b_1 < n^*$ and $b_2 < m^*$. Note that all these properties, except Proposition 3, also hold when $b_1 < n^*$ and $b_2 = m^*$. This implies that Proposition 6, i.e., our (approximate) solution for the network inspection problem $(\mathcal{P})$, and Theorem 3, are still valid when $b_2 = m^*$.

However, most of these properties are not satisfied by the NE of $\Gamma(b_1, b_2)$ when $b_1 < n^*$ and $b_2 > m^*$, as discussed in the following example.

Example 7. Consider the detection model $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \{\mathcal{C}_i,\ i \in \mathcal{V}\})$ defined as follows: Let $\mathcal{V} = \{i_1, \ldots, i_{2n}\}$, with $n \in \mathbb{N}$, and let $\mathcal{E} = \mathcal{E}_1 \cup \{e_1, \ldots, e_n\}$, where $\mathcal{E}_1$ is a discrete set. Then, we define the following monitoring sets: $\forall k \in [\![1, n]\!],\ \mathcal{C}_{i_k} = \mathcal{E}_1 \cup \{e_k\}$ and $\mathcal{C}_{i_{n+k}} = \{e_k\}$.

In this example, $S^{min} = \{i_1, \ldots, i_n\}$ is an MSC, and $T^{max} = \{e_1, \ldots, e_n\}$ is an MSP; so $n^* = m^* = n$. Given any $b_1 < n$ and any $b_2 \in [\![n, |\mathcal{E}_1| + n]\!]$, one can check

that $\forall T \in \mathcal{A}_2 \mid T^{max} \subseteq T,\ (\{i_1, \ldots, i_{b_1}\}, T)$ is a pure NE, whose node basis is not a set cover. Therefore, Proposition 3 does not hold anymore.

Now, if we consider $b_2 = |\mathcal{E}_1| + n$, we just showed that we could construct NE where **P2** can use $n, n+1, \ldots,$ or $n + |\mathcal{E}_1| = b_2$ resources. Thus, (2.18) in Proposition 2 does not hold anymore. This also implies that **P1**'s payoff and the expected detection rate are not constant in equilibrium anymore: We found equilibria where **P1**'s payoff is equal to $b_1, b_1 + 1, \ldots, b_1 + |\mathcal{E}_1|$. This corresponds to equilibrium detection rates equal to $\frac{b_1}{n}, \frac{b_1+1}{n+1}, \ldots, \frac{b_1+|\mathcal{E}_1|}{n+|\mathcal{E}_1|}$, which violates Theorem 3. Since $\frac{b_1+|\mathcal{E}_1|}{n+|\mathcal{E}_1|} \underset{|\mathcal{E}_1|\to+\infty}{\longrightarrow} 1$, the upper bound on the expected detection rates given by Theorem 1 is violated. Furthermore, the bound derived in Theorem 2 is not valid anymore. By choosing $\sigma^1(S^{min}, b_1)$, the expected detection rate may be arbitrarily far from an equilibrium expected detection rate: we can only trivially bound the difference with $1 - \frac{b_1}{n^*}$. $\triangle$

Still, some results remain valid when $b_1 < n^*$ and $b_2 > m^*$: In Proposition 2, (2.17) still holds. In Theorem 1, the lower bound on the equilibrium expected detection rates is still valid. In Theorem 2, when choosing $\sigma^1(S^{min}, b_1)$, the expected detection rate is still guaranteed to be at least $\frac{b_1}{n^*}$, regardless of **P2**'s strategy. From these remaining results, we can show that $b_1' = \lceil \alpha n^* \rceil$ is still a sufficient condition for the expected detection rates in equilibrium to be at least α, and provides an upper bound on the optimal value $b_1^\dagger$ of $(\mathcal{P})$. Furthermore, given an MSC, S^{min}, if **P1** positions these b_1' detectors according to the inspection strategy $\sigma^1(S^{min}, b_1')$, she is still guaranteed to detect a fraction α of the attacks in expectation, regardless of which strategy **P2** chooses.

2.8.2 Summary

In this chapter, we studied a stylized formulation of strategic network inspection in an adversarial environment. In this problem, the defender seeks an inspection strategy that randomizes over minimum-size detector positionings, while ensuring that the expected detection performance against attack plans is above a certain threshold. We formulate the problem as a mathematical program with constraints involving the

mixed strategy NE of a defender-attacker game. Previously known algorithms for equilibrium computation of two-player games cannot be applied to solve this large-scale game. Therefore, we developed a novel approach for analyzing equilibrium properties of this game, which enables us to solve the inspection problem for large-scale networks along with performance guarantees.

Our approach involves: (*i*) deriving useful qualitative properties satisfied by all NE; (*ii*) constructing an $\epsilon-$NE based on solutions of MSC and MSP problems; and (*iii*) computing an approximate solution of the inspection problem that estimates the required number of detectors (with optimality gap), and provides an inspection strategy with guarantee on the expected detection performance. Furthermore, we showed a rather surprising property that, in equilibrium, the expected detection rate and defender strategies can be analyzed by considering a unit attack resource. This property leads to a column generation-based procedure for further improving the guarantees of our solution. Our proofs are based on both game-theoretic and combinatorial ideas; they crucially rely on linear programming duality in zero-sum games, properties of MSC and MSP (including the weak duality between them), and submodularity of the detection model. Our approach can be applied for equilibrium characterization of various security games studied in the literature; importantly, it can be used to solve more generalized models that consider multiple defense and attack resources.

2.9 Proofs of Statements

2.9.1 Preliminary Results

First, we define the following quantities: For a strategy $\sigma^1 \in \Delta(\mathcal{A}_1)$ of **P1**, the *inspection probability* of node $i \in \mathcal{V}$, denoted $\rho_{\sigma^1}(i)$, is the probability with which i is inspected, i.e.:

$$\forall \sigma^1 \in \Delta(\mathcal{A}_1),\ \forall i \in \mathcal{V}, \quad \rho_{\sigma^1}(i) \coloneqq \mathbb{E}_{\sigma^1}\left[\mathbb{1}_{\{i \in S\}}\right] = \sum_{\{S \in \mathcal{A}_1 \,|\, i \in S\}} \sigma^1_S. \tag{2.32}$$

Given a strategy $\sigma^2 \in \Delta(\mathcal{A}_2)$, the *attack probability* of component $e \in \mathcal{E}$, denoted $\rho_{\sigma^2}(e)$, is the probability with which e is targeted by σ^2, i.e.:

$$\forall \sigma^2 \in \Delta(\mathcal{A}_2),\ \forall e \in \mathcal{E}, \quad \rho_{\sigma^2}(e) \coloneqq \mathbb{E}_{\sigma^2}\left[\mathbb{1}_{\{e \in T\}}\right] = \sum_{\{T \in \mathcal{A}_2 \,|\, e \in T\}} \sigma^2_T. \tag{2.33}$$

Lemma 2. *The detection function defined in* (2.1) *satisfies the following properties:*

(i) For any subset of components $T \in 2^{\mathcal{E}}$, $\mathrm{F}(\cdot, T)$ is submodular and monotone:

$$\forall T \in 2^{\mathcal{E}},\ \forall (S, S') \in (2^{\mathcal{V}})^2 :$$
$$\mathrm{F}(S \cup S', T) + \mathrm{F}(S \cap S', T) \leq \mathrm{F}(S, T) + \mathrm{F}(S', T), \tag{2.34}$$
$$S \subseteq S' \implies \mathrm{F}(S, T) \leq \mathrm{F}(S', T). \tag{2.35}$$

(ii) For any detector positioning $S \in 2^{\mathcal{V}}$, $\mathrm{F}(S, \cdot)$ is finitely additive:

$$\forall S \in 2^{\mathcal{V}},\ \forall (T, T') \in (2^{\mathcal{E}})^2 \mid T \cap T' = \emptyset, \quad \mathrm{F}(S, T \cup T') = \mathrm{F}(S, T) + \mathrm{F}(S, T'). \tag{2.36}$$

Proof of Lemma 2.

(i) Consider a subset of components $T \in 2^{\mathcal{E}}$, and a pair of detector positionings $(S, S') \in (2^{\mathcal{V}})^2$. Then, $\mathcal{C}_{S \cup S'} = \mathcal{C}_S \cup \mathcal{C}_{S'}$ and $\mathcal{C}_{S \cap S'} \subseteq \mathcal{C}_S \cap \mathcal{C}_{S'}$, and we obtain:

$$\begin{aligned}
\mathrm{F}(S \cup S', T) + \mathrm{F}(S \cap S', T) &\overset{(2.1)}{=} |\mathcal{C}_{S \cup S'} \cap T| + |\mathcal{C}_{S \cap S'} \cap T| \\
&= |(\mathcal{C}_S \cap T) \cup (\mathcal{C}_{S'} \cap T)| + |\mathcal{C}_{S \cap S'} \cap T| \\
&= |\mathcal{C}_S \cap T| + |\mathcal{C}_{S'} \cap T| - |\mathcal{C}_S \cap \mathcal{C}_{S'} \cap T| + |\mathcal{C}_{S \cap S'} \cap T| \\
&\leq |\mathcal{C}_S \cap T| + |\mathcal{C}_{S'} \cap T| \overset{(2.1)}{=} \mathrm{F}(S, T) + \mathrm{F}(S', T).
\end{aligned}$$

Furthermore, if $S \subseteq S'$, then: $\mathrm{F}(S, T) \overset{(2.1)}{=} |\mathcal{C}_S \cap T| \leq |\mathcal{C}_{S'} \cap T| \overset{(2.1)}{=} \mathrm{F}(S', T)$.

(ii) Consider a detector positioning $S \in 2^{\mathcal{V}}$. Then:

$$\begin{aligned}\forall (T,T') \in (2^{\mathcal{E}})^2 \mid T \cap T' = \emptyset, \quad \mathrm{F}(S, T \cup T') &\overset{(2.1)}{=} |\mathcal{C}_S \cap (T \cup T')| \\ &= |\mathcal{C}_S \cap T| + |\mathcal{C}_S \cap T'| - |\mathcal{C}_S \cap T \cap T'| \\ &\overset{(2.1)}{=} \mathrm{F}(S,T) + \mathrm{F}(S,T').\end{aligned}$$

□

Corollary 2. *The detection function defined in* (2.1) *satisfies the following properties:*

$$\forall (S,T) \in 2^{\mathcal{V}} \times 2^{\mathcal{E}},\ \mathrm{F}(S,T) \leq \sum_{i \in S} \mathrm{F}(i,T), \tag{2.37}$$

$$\forall (S,T) \in 2^{\mathcal{V}} \times 2^{\mathcal{E}},\ \mathrm{F}(S,T) = \sum_{e \in T} \mathrm{F}(S,e). \tag{2.38}$$

Proof of Corollary 2.

(i) Consider $T \in 2^{\mathcal{E}}$. Since $\mathrm{F}(\cdot, T)$ is a submodular and nonnegative function, then $\mathrm{F}(\cdot, T)$ is subadditive, i.e., $\forall (S,S') \in (2^{\mathcal{V}})^2,\ \mathrm{F}(S \cup S', T) \leq \mathrm{F}(S,T) + \mathrm{F}(S',T)$. Therefore, by induction, we obtain:

$$\forall S \in 2^{\mathcal{V}},\ \mathrm{F}(S,T) = \mathrm{F}(\cup_{i \in S}\{i\}, T) \leq \sum_{i \in S} \mathrm{F}(i,T).$$

(ii) Consider $S \in 2^{\mathcal{V}}$. Since $\mathrm{F}(S, \cdot)$ is additive (Lemma 2), we obtain by induction that:

$$\forall T \in 2^{\mathcal{E}},\ \mathrm{F}(S,T) = \mathrm{F}(S, \cup_{e \in T}\{e\}) \overset{(2.36)}{=} \sum_{e \in T} \mathrm{F}(S,e).$$

□

Lemma 3. *Given an inspection strategy $\sigma^1 \in \Delta(\mathcal{A}_1)$, let $\{i_1, \ldots, i_n\} \in 2^{\mathcal{V}}$ denote a set that contains its node basis $\mathcal{V}_{\sigma^1}$ and such that $\rho_{\sigma^1}(i_1) \leq \cdots \leq \rho_{\sigma^1}(i_n)$. Then, we*

have the following inequality:

$$\forall b \in [\![1, n]\!],\ \sum_{k=1}^{b} \rho_{\sigma^1}(i_k) \leq \frac{b}{n} \mathbb{E}_{\sigma^1}[|S|]. \tag{2.39}$$

Similarly, given an attack strategy $\sigma^2 \in \Delta(\mathcal{A}_2)$, let $\{e_1, \ldots, e_m\} \in 2^{\mathcal{E}}$ denote a set that contains its component basis $\mathcal{E}_{\sigma^2}$, and such that $\rho_{\sigma^2}(e_1) \geq \cdots \geq \rho_{\sigma^2}(e_m)$. Then, we have the following inequality:

$$\forall b \in [\![1, m]\!],\ \sum_{l=1}^{b} \rho_{\sigma^2}(e_l) \geq \frac{b}{m} \mathbb{E}_{\sigma^2}[|T|]. \tag{2.40}$$

Proof of Lemma 3. Consider an inspection strategy $\sigma^1 \in \Delta(\mathcal{A}_1)$, and a set of nodes $\{i_1, \ldots, i_n\} \in 2^{\mathcal{V}}$ such that $\mathcal{V}_{\sigma^1} \subseteq \{i_1, \ldots, i_n\}$ and $\rho_{\sigma^1}(i_1) \leq \cdots \leq \rho_{\sigma^1}(i_n)$. We show the result by contradiction: let us assume that $\exists\, b \in [\![1, n]\!] \mid \sum_{k=1}^{b} \rho_{\sigma^1}(i_k) > \frac{b}{n} \mathbb{E}_{\sigma^1}[|S|]$.

First, we can deduce the following inequality:

$$\rho_{\sigma^1}(i_b) = \frac{1}{b} \sum_{k=1}^{b} \rho_{\sigma^1}(i_b) \geq \frac{1}{b} \sum_{k=1}^{b} \rho_{\sigma^1}(i_k) > \frac{b \mathbb{E}_{\sigma^1}[|S|]}{bn} = \frac{\mathbb{E}_{\sigma^1}[|S|]}{n}. \tag{2.41}$$

Besides, since $\mathcal{V}_{\sigma^1} \subseteq \{i_1, \ldots, i_n\}$, then $\forall S \in \text{supp}(\sigma^1),\ S \subseteq \{i_1, \ldots, i_n\}$ and we have the following equality: $\forall S \in \text{supp}(\sigma^1),\ |S| = \sum_{k=1}^{n} \mathbb{1}_{\{i_k \in S\}}$. This enables us to obtain the following contradiction:

$$\begin{aligned} \mathbb{E}_{\sigma^1}[|S|] = \sum_{k=1}^{n} \mathbb{E}_{\sigma^1}[\mathbb{1}_{\{i_k \in S\}}] &\overset{(2.32)}{=} \sum_{k=1}^{b} \rho_{\sigma^1}(i_k) + \sum_{b+1}^{n} \rho_{\sigma^1}(i_k) \\ &> \frac{b \mathbb{E}_{\sigma^1}[|S|]}{n} + (n-b) \rho_{\sigma^1}(i_b) \overset{(2.41)}{>} \mathbb{E}_{\sigma^1}[|S|]. \end{aligned}$$

Therefore, $\forall b \in [\![1, n]\!],\ \sum_{k=1}^{b} \rho_{\sigma^1}(i_k) \leq \frac{b}{n} \mathbb{E}_{\sigma^1}[|S|]$. (2.40) can be analogously proved. □

Lemma 4. *Γ is strategically equivalent to the game $\widetilde{\Gamma} \coloneqq \langle \{1, 2\}, (\Delta(\mathcal{A}_1), \Delta(\mathcal{A}_2)), (-U_2, U_2) \rangle$.*

Proof of Lemma 4. Adding a term to **P1**'s payoff that only depends on **P2**'s action

does not change the NE of the game. Thus, the following transformation preserves the set of NE:

$$\forall (S,T) \in \mathcal{A}_1 \times \mathcal{A}_2,\ u_1(S,T) - |T| = \mathrm{F}(S,T) - |T| = -u_2(S,T). \tag{2.42}$$

So $\Gamma(b_1, b_2)$ and $\widetilde{\Gamma}(b_1, b_2)$ are strategically equivalent, and have the same set of NE $\Sigma(b_1, b_2)$. □

Lemma 5. *The size of MSPs is no greater than the size of MSCs, i.e., $m^* \leq n^*$.*

Proof of Lemma 5. Consider an MSP $T^{max} = \{e_1, \ldots, e_{m^*}\} \in \mathcal{M}$ and an MSC $S^{min} = \{i_1, \ldots, i_{n^*}\} \in \mathcal{S}$. Then, we have the desired inequality:

$$\begin{aligned} m^* &\overset{(2.11)}{=} \sum_{l=1}^{m^*} \mathrm{F}(S^{min}, e_l) \overset{(2.37)}{\leq} \sum_{l=1}^{m^*} \sum_{k=1}^{n^*} \mathrm{F}(i_k, e_l) \\ &= \sum_{k=1}^{n^*} \sum_{l=1}^{m^*} \mathrm{F}(i_k, e_l) \overset{(2.38)}{=} \sum_{k=1}^{n^*} \mathrm{F}(i_k, T^{max}) \overset{(2.12)}{\leq} n^*. \end{aligned}$$

□

2.9.2 Proofs of Section 2.3

Lemma 6. *Consider a set of nodes $S = \{i_1, \ldots, i_n\} \in 2^{\mathcal{V}}$ of size $n \geq b_1$, and a set of components $T = \{e_1, \ldots, e_m\} \in 2^{\mathcal{E}}$ of size $m \geq b_2$. We define the following pure actions:*

$$\forall k \in [\![1, n]\!],\ S^k = \begin{cases} \{i_k, \ldots, i_{k+b_1-1}\} & \text{if } \ k \leq n - b_1 + 1, \\ \{i_k, \ldots, i_n, i_1, \ldots, i_{k+b_1-n-1}\} & \text{if } \ k \geq n - b_1 + 2, \end{cases} \tag{2.43}$$

$$\forall l \in [\![1, m]\!],\ T^l = \begin{cases} \{e_l, \ldots, e_{l+b_2-1}\} & \text{if } \ l \leq m - b_2 + 1, \\ \{e_l, \ldots, e_m, e_1, \ldots, e_{l+b_2-m-1}\} & \text{if } \ l \geq m - b_2 + 2, \end{cases} \tag{2.44}$$

and a strategy profile $(\sigma^1(S,b_1),\sigma^2(T,b_2)) \in \Delta(\mathcal{A}_1)\times\Delta(\mathcal{A}_2)$ *supported over* $\{S^1,\ldots,S^n\}$ *and* $\{T^1,\ldots,T^m\}$*, where:*

$$\forall k \in [\![1,n]\!],\ \sigma^1(S,b_1)_{S^k} \coloneqq \frac{1}{n}, \tag{2.45}$$

$$\forall l \in [\![1,m]\!],\ \sigma^2(T,b_2)_{T^l} \coloneqq \frac{1}{m}. \tag{2.46}$$

Then, the strategy profile $(\sigma^1(S,b_1),\sigma^2(T,b_2))$ *has the following properties:*

(i) Each node in S *(resp. each component in* T*) is inspected (resp. targeted) with an identical probability given by:*

$$\forall i \in S,\ \rho_{\sigma^1(S,b_1)}(i) = \frac{b_1}{n}, \tag{2.47}$$

$$\forall e \in T,\ \rho_{\sigma^2(T,b_2)}(e) = \frac{b_2}{m}. \tag{2.48}$$

(ii) Each node in S *(resp. each component in* T*) belongs to* b_1 *actions (resp.* b_2 *actions) in the support of* $\sigma^1(S,b_1)$ *(resp.* $\sigma^2(T,b_2)$*):*

$$\forall i \in S,\ |\{k \in [\![1,n]\!] \mid i \in S^k\}| = b_1, \tag{2.49}$$

$$\forall e \in T,\ |\{l \in [\![1,m]\!] \mid e \in T^l\}| = b_2. \tag{2.50}$$

(iii) The following inequality is satisfied:

$$\forall e \in \mathcal{E},\ \mathrm{F}(S,e) \le \frac{1}{b_1}\sum_{k=1}^{n}\mathrm{F}(S^k,e). \tag{2.51}$$

Proof of Lemma 6. We show the result for a set of nodes $S \in 2^{\mathcal{V}}$ of size $n \ge b_1$. First we note, by construction, that each node $i \in S$ belongs to the same number of detector positionings S^k, $k \in [\![1,n]\!]$. Thus, (2.49) follows from the following calculations:

$$\begin{aligned} nb_1 &\overset{(2.43)}{=} \sum_{k=1}^{n}\sum_{i'\in\mathcal{V}} \mathbb{1}_{\{i'\in S^k\}} = \sum_{i'\in\mathcal{V}} |\{k \in [\![1,n]\!] \mid i' \in S^k\}| \\ &= n \times |\{k \in [\![1,n]\!] \mid i \in S^k\}|, \quad \forall i \in S. \end{aligned}$$

Then, we can show (2.47). For every node $i \in S$, we have:

$$\rho_{\sigma^1(S,b_1)}(i) \overset{(2.32)}{=} \sum_{k=1}^{n} \sigma^1(S,b_1)_{S^k} \mathbb{1}_{\{i \in S^k\}} \overset{(2.45)}{=} \frac{1}{n} \sum_{k=1}^{n} \mathbb{1}_{\{i \in S^k\}}$$
$$= \frac{1}{n} |\{k \in [\![1,n]\!] \mid i \in S^k\}| \overset{(2.49)}{=} \frac{b_1}{n}.$$

An analogous proof can be applied to $T \in 2^{\mathcal{E}}$ of size $m \geq b_2$ to show (2.48) and (2.50).

Finally, let us show (2.51). Consider $e \in \mathcal{E}$.

- If $\mathrm{F}(S,e) = 1$, then $\exists\, i_0 \in S \mid \mathrm{F}(i_0,e) = 1$. Since there are b_1 detector positionings in $\{S^k,\ k \in [\![1,n]\!]\}$ that contain i_0, then $\frac{1}{b_1} \sum_{k=1}^{n} \mathrm{F}(S^k,e) \geq 1 = \mathrm{F}(S,e)$.
- If $\mathrm{F}(S,e) = 0$, then $\forall i \in S$, $\mathrm{F}(i,e) = 0$ and $\frac{1}{b_1} \sum_{k=1}^{n} \mathrm{F}(S^k,e) = 0$.

Note that (2.51) can also be derived from a property of the detection function. Since $\forall T \in 2^{\mathcal{E}}$, $\mathrm{F}(\cdot,T)$ is submodular, monotone and nonnegative (Lemma 2), then it is fractionally subadditive [33]. Inequality (2.51) is then a direct application of this property combined with (2.49). □

Proof of Proposition 1. We show that (i) given a minimal set cover $S' \in 2^{\mathcal{V}}$, the optimal value of $(\mathrm{LP}_{S'})$ is $b_2 \left(\frac{b_1}{|S'|} - 1\right)$, and an optimal solution is given by $\sigma^1(S',b_1)$. Then, we show that (ii) given a set packing $T' \in 2^{\mathcal{E}}$ of size at least b_2, the optimal value of $(\mathrm{LP}_{T'})$ is $\max\left\{0, b_2\left(1 - \frac{b_1}{|T'|}\right)\right\}$, and an optimal solution is given by $\sigma^2(T',b_2)$.

(i) Consider a minimal set cover $S' = \{i_1,\ldots,i_n\} \in 2^{\mathcal{V}}$ of size n. Necessarily, S' is such that:

$$\forall k \in [\![1,n]\!],\ \exists\, e_k \in \mathcal{E} \mid \mathrm{F}(i_k,e_k) = 1 \text{ and } \mathrm{F}(i_j,e_k) = 0, \quad \forall j \neq k. \tag{2.52}$$

– First, let us demonstrate that $\max_{\{\sigma^1 \in \Delta(\mathcal{A}_1) \mid \mathcal{V}_{\sigma^1} \subseteq S'\}} \min_{T \in \mathcal{A}_2} -U_2(\sigma^1,T) \geq b_2\left(\frac{b_1}{n} - 1\right)$. Consider $\sigma^1(S',b_1) \in \Delta(\mathcal{A}_1)$ defined in (2.45). Recall that $\sigma^1(S',b_1)$ is such that $\mathcal{V}_{\sigma^1(S',b_1)} = S'$ and $\forall k \in [\![1,n]\!]$, $\rho_{\sigma^1(S',b_1)}(i_k) = \frac{b_1}{n}$. Also, recall that we are in the case when $b_1 < n^*$, implying that $b_1 < n^* \leq n$.

Since S' is a set cover, then $\forall e \in \mathcal{E},\ \exists\, k_e \in [\![1, n]\!] \mid \mathrm{F}(i_{k_e}, e) = 1$. Furthermore, F is a nonnegative function. Therefore:

$$\forall e \in \mathcal{E},\ \sum_{S \in \mathcal{A}_1} \sigma^1(S', b_1)_S \,\mathrm{F}(S, e) \overset{(2.35)}{\geq} \sum_{\{S \in \mathcal{A}_1 \,|\, i_{k_e} \in S\}} \sigma^1(S', b_1)_S \overset{(2.32)}{=} \rho_{\sigma^1(S', b_1)}(i_{k_e}) \overset{(2.47)}{=} \frac{b_1}{n}. \tag{2.53}$$

Thus, we obtain:

$$\begin{aligned} \forall T \in \mathcal{A}_2,\ -U_2(\sigma^1(S', b_1), T) &\overset{(2.3)}{=} \sum_{S \in \mathcal{A}_1} \sigma^1(S', b_1)_S \,\mathrm{F}(S, T) - |T| \\ &\overset{(2.38)}{=} \sum_{e \in T} \sum_{S \in \mathcal{A}_1} \sigma^1(S', b_1)_S \,\mathrm{F}(S, e) - |T| \\ &\overset{(2.53)}{\geq} \sum_{e \in T} \frac{b_1}{n} - |T| = \underbrace{\left(\frac{b_1}{n} - 1\right)}_{<0} \underbrace{|T|}_{\leq b_2} \\ &\geq b_2 \left(\frac{b_1}{n} - 1\right). \end{aligned} \tag{2.54}$$

Therefore:

$$\begin{aligned} \max_{\{\sigma^1 \in \Delta(\mathcal{A}_1) \,|\, \mathcal{V}_{\sigma^1} \subseteq S'\}} \min_{T \in \mathcal{A}_2} -U_2(\sigma^1, T) &\geq \min_{T \in \mathcal{A}_2} -U_2(\sigma^1(S', b_1), T) \\ &\geq b_2 \left(\frac{b_1}{n} - 1\right). \end{aligned} \tag{2.55}$$

Note that the only property of $\sigma^1(S', b_1)$ that was used to show (2.55) is that its node basis is S' and that $\forall i \in S',\ \rho_{\sigma^1(S', b_1)}(i) = \frac{b_1}{n}$.

– Now, let us show the reverse inequality. Consider any $\sigma^1 \in \Delta(\mathcal{A}_1)$ such that $\mathcal{V}_{\sigma^1} \subseteq S' = \{i_1, \ldots, i_n\}$. Let us reorder the indices such that $\rho_{\sigma^1}(i_1) \leq \cdots \leq \rho_{\sigma^1}(i_n)$.

Consider $T' = \{e_1, \ldots, e_{b_2}\}$ (where the e_k's are defined in (2.52)). Then, for

every $k \in [\![1, b_2]\!]$:

$$\mathbb{E}_{\sigma^1}[\mathrm{F}(S, e_k)] \overset{(2.52)}{=} \sum_{\{S \in \mathcal{A}_1 \,|\, i_k \in S\}} \sigma^1_S \underbrace{\mathrm{F}(S, e_k)}_{=1} + \sum_{\{S \in \mathcal{A}_1 \,|\, i_k \notin S\}} \underbrace{\sigma^1_S \, \mathrm{F}(S, e_k)}_{=0}$$
$$\overset{(2.32)}{=} \rho_{\sigma^1}(i_k), \tag{2.56}$$

where we combined the fact that the node basis of σ^1 is a subset of S' and that i_k is the only node from S' that monitors component e_k (by construction). This implies that:

$$\min_{T \in \mathcal{A}_2} -U_2(\sigma^1, T) \leq -U_2(\sigma^1, T') \overset{(2.3)}{=} \mathbb{E}_{\sigma^1}[\mathrm{F}(S, T')] - |T'|$$
$$\overset{(2.38),(2.56)}{=} \sum_{k=1}^{b_2} \rho_{\sigma^1}(i_k) - b_2 \overset{(2.39)}{\leq} b_2 \left(\frac{b_1}{n} - 1 \right).$$

This upper bound holds for any $\sigma^1 \in \Delta(\mathcal{A}_1)$ such that $\mathcal{V}_{\sigma^1} \subseteq S'$, and does not depend on σ^1. Therefore, $\max_{\{\sigma^1 \in \Delta(\mathcal{A}_1) \,|\, \mathcal{V}_{\sigma^1} \subseteq S'\}} \min_{T \in \mathcal{A}_2} -U_2(\sigma^1, T) \leq b_2 \left(\frac{b_1}{n} - 1 \right)$, and we can conclude that:

$$\max_{\{\sigma^1 \in \Delta(\mathcal{A}_1) \,|\, \mathcal{V}_{\sigma^1} \subseteq S'\}} \min_{T \in \mathcal{A}_2} -U_2(\sigma^1, T) = \min_{T \in \mathcal{A}_2} -U_2(\sigma^1(S', b_1), T) = b_2 \left(\frac{b_1}{n} - 1 \right).$$

The optimal value of $(\mathrm{LP}_{S'})$ is $b_2 \left(\frac{b_1}{n} - 1 \right)$, and an optimal solution is given by $\sigma^1(S', b_1)$.

(ii) Consider a set packing $T' = \{e_1, \ldots, e_m\} \in 2^{\mathcal{E}}$ of size $m \geq b_2$.

Case 1: If $b_1 \geq m$, then **P1** can monitor all the components of T' with a single detector positioning S'. Therefore, the optimal value of $(\mathrm{LP}_{T'})$ in this case is equal to $0 = \max\{0, b_2(1 - \frac{b_1}{m})\}$.

Case 2: Consider $b_1 < m$. In this case, note that $\max\{0, b_2(1 - \frac{b_1}{m})\} = b_2(1 - \frac{b_1}{m})$.

– First, we show that $\max_{\{\sigma^2 \in \Delta(\mathcal{A}_2) \,|\, \mathcal{E}_{\sigma^2} \subseteq T'\}} \min_{S \in \mathcal{A}_1} U_2(S, \sigma^2) \geq b_2 \left(1 - \frac{b_1}{m}\right)$. Consider $\sigma^2(T', b_2) \in \Delta(\mathcal{A}_2)$ defined in (2.46). Since T' is a set packing, then

$\forall i \in \mathcal{V},\ \mathrm{F}(i, T') \leq 1$. This implies that:

$$\begin{aligned}
\forall S \in \mathcal{A}_1,\ U_2(S, \sigma^2(T', b_2)) &\overset{(2.3)}{=} \mathbb{E}_{\sigma^2(T', b_2)}[|T| - \mathrm{F}(S, T)] \\
&\overset{(2.37),(2.44)}{\geq} b_2 - \sum_{i \in S} \mathbb{E}_{\sigma^2(T', b_2)}[\mathrm{F}(i, T)] \\
&\overset{(2.33),(2.38)}{=} b_2 - \sum_{i \in S} \sum_{e \in \mathcal{E}} \mathrm{F}(i, e) \rho_{\sigma^2(T', b_2)}(e) \\
&\overset{(2.38),(2.48)}{=} b_2 - \frac{b_2}{m} \sum_{i \in S} \underbrace{\mathrm{F}(i, T')}_{\leq 1} \geq b_2 \left(1 - \frac{b_1}{m}\right).
\end{aligned}$$

Therefore:

$$\begin{aligned}
\max_{\{\sigma^2 \in \Delta(\mathcal{A}_2) \,|\, \mathcal{E}_{\sigma^2} \subseteq T'\}} \min_{S \in \mathcal{A}_1} U_2(S, \sigma^2) &\geq \min_{S \in \mathcal{A}_1} U_2(S, \sigma^2(T', b_2)) \\
&\geq b_2 \left(1 - \frac{b_1}{m}\right). \qquad (2.57)
\end{aligned}$$

Similarly, the only property of $\sigma^2(T', b_2)$ that was used to show (2.57) is that its component basis is T' and that $\forall e \in T',\ \rho_{\sigma^2(T', b_2)}(e) = \frac{b_2}{m}$.

– Now, let us show the reverse inequality. Consider any $\sigma^2 \in \Delta(\mathcal{A}_2) \mid \mathcal{E}_{\sigma^2} \subseteq T' = \{e_1, \ldots, e_m\}$. Let us reorder the indices such that $\rho_{\sigma^2}(e_1) \geq \cdots \geq \rho_{\sigma^2}(e_m)$. In Section 2.2.2, we assumed that each component can be monitored from at least one node. Therefore $\forall l \in [\![1, m]\!],\ \exists\, i_l \in \mathcal{V} \mid\ \mathrm{F}(i_l, e_l) = 1$ (note that the i_l's are distinct since T' is a set packing). Now, consider the detector positioning

$S' = \{i_1, \ldots, i_{b_1}\}$. S' monitors $\{e_1, \ldots, e_{b_1}\}$, which enables us to show:

$$\begin{aligned}
\min_{S\in\mathcal{A}_1} U_2(S,\sigma^2) \leq U_2(S',\sigma^2) &\overset{(2.3),(2.38)}{=} \mathbb{E}_{\sigma^2}[|T|] - \mathbb{E}_{\sigma^2}[\sum_{e\in T} \mathrm{F}(S',e)] \\
&\overset{(2.33)}{=} \mathbb{E}_{\sigma^2}[|T|] - \sum_{e\in\mathcal{E}} \mathrm{F}(S',e)\rho_{\sigma^2}(e) \\
&= \mathbb{E}_{\sigma^2}[|T|] - \sum_{l=1}^{b_1} \underbrace{\mathrm{F}(S',e_l)}_{=1}\rho_{\sigma^2}(e_l) - \sum_{l=b_1+1}^{m} \underbrace{\mathrm{F}(S',e_l)\rho_{\sigma^2}(e_l)}_{\geq 0} \\
&\overset{(2.40)}{\leq} \underbrace{\left(1-\frac{b_1}{m}\right)}_{>0} \underbrace{\mathbb{E}_{\sigma^2}[|T|]}_{\leq b_2} \leq \left(1-\frac{b_1}{m}\right) b_2.
\end{aligned}$$

This upper bound is valid for any $\sigma^2 \in \Delta(\mathcal{A}_2)$ such that $\mathcal{E}_{\sigma^2} \subseteq T'$, and does not depend on σ^2. Therefore, $\max_{\{\sigma^2\in\Delta(\mathcal{A}_2)\,|\,\mathcal{E}_{\sigma^2}\subseteq T'\}} \min_{S\in\mathcal{A}_1} U_2(S,\sigma^2) \leq b_2\left(1-\frac{b_1}{m}\right)$, and we can conclude that:

$$\max_{\{\sigma^2\in\Delta(\mathcal{A}_2)\,|\,\mathcal{E}_{\sigma^2}\subseteq T'\}} \min_{S\in\mathcal{A}_1} U_2(S,\sigma^2) = \min_{S\in\mathcal{A}_1} U_2(S,\sigma^2(T',b_2)) = b_2\left(1-\frac{b_1}{m}\right).$$

The optimal value of $(\mathrm{LP}_{T'})$ in this case ($b_1 < m$) is $b_2\left(1-\frac{b_1}{m}\right) = \max\{0, b_2\left(1-\frac{b_1}{m}\right)\}$, and an optimal solution is given by $\sigma^2(T',b_2)$.

□

Proof of Proposition 2.

(i.a) First, let us show by contradiction that **P1** uses all her resources in equilibrium. Suppose that $\exists\,(\sigma^{1^*},\sigma^{2^*}) \in \Sigma,\ \exists\, S^0 \in \mathrm{supp}(\sigma^{1^*}) \mid |S^0| < b_1$.

– The first step is to show that **P2**'s strategy σ^{2^*} necessarily targets with positive probability at least one component that is not monitored by S^0. On the contrary, assume that $\forall e \in \mathcal{E}:\ \rho_{\sigma^{2^*}}(e) > 0 \implies \mathrm{F}(S^0,e) = 1$. Then, **P1** can detect all the attacks of σ^{2^*} with the detector positioning S^0. Thus, S^0 is a best response for **P1** to σ^{2^*}, and **P2**'s payoff in equilibrium is 0. Since **P2**'s payoff is identical for any NE (direct consequence of Lemma 4), then **P2**'s

payoff for the initial NE we considered, $(\sigma^{1^*}, \sigma^{2^*})$, is also 0. However, since $b_1 < n^*$, we know that $\exists\, e' \in \mathcal{E} \mid \mathrm{F}(S^0, e') = 0$, i.e., e' is not monitored by S^0. Since $S^0 \in \mathrm{supp}(\sigma^{1^*})$, then e' is not monitored with positive probability. Therefore, if **P2** targets e', she will get a positive payoff, which contradicts the equilibrium condition (2.5) for $(\sigma^{1^*}, \sigma^{2^*})$. Therefore, $\exists\, e_0 \in \mathcal{E} \mid \rho_{\sigma^{2^*}}(e_0) > 0$ and $\mathrm{F}(S^0, e_0) = 0$.

– Now, we can show that **P1** can increase her payoff by placing one more detector. Let us denote $i_0 \in \mathcal{V} \backslash S^0$ that satisfies $\mathrm{F}(i_0, e_0) = 1$. Then, by considering the detector positioning $S' = S^0 \cup \{i_0\} \in \mathcal{A}_1$, we obtain:

$$
\begin{aligned}
U_1(S', \sigma^{2^*}) &\overset{(2.2),(2.38)}{=} \mathbb{E}_{\sigma^{2^*}}[\sum_{e \in \mathcal{E}} \mathrm{F}(S', e) \mathbb{1}_{\{e \in T\}}] \\
&\overset{(2.33)}{=} \rho_{\sigma^{2^*}}(e_0) + \sum_{e \in \mathcal{E} \backslash \{e_0\}} \mathrm{F}(S', e) \rho_{\sigma^{2^*}}(e) \\
&\overset{(2.35)}{\geq} \rho_{\sigma^{2^*}}(e_0) + \sum_{e \in \mathcal{E} \backslash \{e_0\}} \mathrm{F}(S^0, e) \rho_{\sigma^{2^*}}(e) \\
&\overset{(2.2)}{=} \underbrace{\rho_{\sigma^{2^*}}(e_0)}_{>0} + U_1(S^0, \sigma^{2^*}) \\
&> U_1(S^0, \sigma^{2^*}),
\end{aligned}
$$

which violates the equilibrium condition (2.4) for $(\sigma^{1^*}, \sigma^{2^*})$. Therefore, $\forall S \in \mathrm{supp}(\sigma^{1^*}),\ |S| = b_1$.

(i.b) Now, let us show that **P2** uses all her resources in equilibrium. By contradiction, suppose that $\exists\, (\sigma^{1^*}, \sigma^{2^*}) \in \Sigma,\ \exists\, T^0 \in \mathrm{supp}(\sigma^{2^*}) \mid |T^0| < b_2$.

– The first step is to show that there exists a component e' not in T^0 that is not monitored by every detector positioning in the support of σ^{1^*}. Let us assume the contrary, i.e., that $\forall S \in \mathrm{supp}(\sigma^{1^*}),\ \forall e \notin T^0,\ \mathrm{F}(S, e) = 1$. First, let us denote $T^1 \subseteq T^0$ the subset of components of T^0 that are unmonitored by at least one detector positioning $S \in \mathrm{supp}(\sigma^{1^*})$, i.e., $T^1 \coloneqq \bigcup_{S \in \mathrm{supp}(\sigma^{1^*})} (\mathcal{E} \backslash \mathcal{C}_S) \subseteq T^0$.

For all $S \in \mathrm{supp}(\sigma^{1^*})$, let k_S denote the number of components of T^1 that

are not monitored by S. Since every component outside of T^1 is monitored by every detector positioning in the support of σ^{1^*}, then **P2**'s best response to σ^{1^*} is any attack plan $T \in \mathcal{A}_2$ such that $T^1 \subseteq T$ (note that $|T^1| \leq b_2$), and **P2**'s equilibrium payoff is equal to $k^* \coloneqq \mathbb{E}_{\sigma^{1^*}}[k_S]$. This is shown in the following steps:

$$\begin{aligned}\forall T \in \mathcal{A}_2 \mid T^1 \subseteq T,\ U_2(\sigma^{1^*}, T) &\overset{(2.3),(2.36)}{=} |T| - \mathbb{E}_{\sigma^{1^*}}[\mathrm{F}(S, T^1)] - \mathbb{E}_{\sigma^{1^*}}[\mathrm{F}(S, T \backslash T^1)] \\ &= |T| - \mathbb{E}_{\sigma^{1^*}}[|T^1| - k_S] - \mathbb{E}_{\sigma^{1^*}}[|T \backslash T^1|] \\ &= \mathbb{E}_{\sigma^{1^*}}[k_S].\end{aligned}$$

Thus, **P1**'s equilibrium payoff in the zero-sum game $\widetilde{\Gamma}$ is equal to $-k^*$. From Proposition 1, we know that $-k^* \geq b_2 \left(\frac{b_1}{n^*} - 1\right)$. Since we are in the case when $b_2 < m^*$, and we have $m^* \leq n^*$ (Lemma 5), then we obtain:

$$k^* \leq \frac{b_2}{n^*}(n^* - b_1) < \frac{m^*}{n^*}(n^* - b_1) \leq n^* - b_1. \tag{2.58}$$

Consider $S \in \mathrm{supp}(\sigma^{1^*})$. We know that S leaves k_S network components unmonitored, that we denote $e_1, \ldots, e_{k_S}$. For $l \in [\![1, k_S]\!]$, let i_l be a node from where a detector can monitor component e_l. Then, $S \cup \{i_1, \ldots, i_{k_S}\}$ is a set cover (of size at most $b_1 + k_S$). By definition of n^*, we deduce that $b_1 + k_S \geq n^*$. Therefore, $\forall S \in \mathrm{supp}(\sigma^{1^*}),\ k_S \geq n^* - b_1$. This last result implies that $k^* = \mathbb{E}_{\sigma^{1^*}}[k_S] \geq n^* - b_1$, which contradicts (2.58). Thus, $\exists\, (e', S') \in \mathcal{E} \backslash T^0 \times \mathrm{supp}(\sigma^{1^*}) \mid \mathrm{F}(S', e') = 0$.

– Now, we can show that **P2** can increase her payoff by targeting component e' and the components in T^0. Let $T' = T^0 \cup \{e'\} \in \mathcal{A}_2$ (since $|T^0| < b_2$). Then,

we get:

$$U_2(\sigma^{1^*}, T') - U_2(\sigma^{1^*}, T^0) \overset{(2.3),(2.36)}{=} 1 - \mathbb{E}_{\sigma^{1^*}}[\mathrm{F}(S, e')] = \mathbb{E}_{\sigma^{1^*}}[\underbrace{1 - \mathrm{F}(S, e')}_{\geq 0}]$$

$$\geq \underbrace{\sigma^{1^*}_{S'}}_{>0}(1 - \underbrace{\mathrm{F}(S, e')}_{=0}) > 0,$$

which is a contradiction. Therefore, $\forall T \in \mathrm{supp}(\sigma^{2^*}),\ |T| = b_2$.

(ii) Finally, we show that **P1**'s strategies in equilibrium are the optimal solutions of $(\overline{\mathrm{LP}_1})$. First, from (i), we can deduce that the set of optimal solutions of (LP_1) is a subset of $\Delta(\overline{\mathcal{A}_1})$. Therefore, the equilibrium inspection strategies are the optimal solutions of $\max_{\sigma^1 \in \Delta(\overline{\mathcal{A}_1})} \min_{T \in \mathcal{A}_2} -U_2(\sigma^1, T)$.

Now, consider an inspection strategy $\sigma^1 \in \Delta(\overline{\mathcal{A}_1})$. Since $\overline{\mathcal{A}_2} \subseteq \mathcal{A}_2$, then we trivially have $\min_{T \in \mathcal{A}_2} -U_2(\sigma^1, T) \leq \min_{T \in \overline{\mathcal{A}_2}} -U_2(\sigma^1, T)$. To obtain the reverse inequality, let $T^0 \in \mathcal{A}_2$ be an attack plan that satisfies $T^0 \in \arg\min_{T \in \mathcal{A}_2} -U_2(\sigma^1, T)$. Then, consider $T' \in \overline{\mathcal{A}_2} \mid T^0 \subseteq T'$. We can deduce that:

$$\min_{T \in \mathcal{A}_2} -U_2(\sigma^1, T) = -U_2(\sigma^1, T^0) \geq -U_2(\sigma^1, T') \geq \min_{T \in \overline{\mathcal{A}_2}} -U_2(\sigma^1, T).$$

Therefore, $\forall \sigma^1 \in \Delta(\overline{\mathcal{A}_1})$, $\min_{T \in \mathcal{A}_2} -U_2(\sigma^1, T) = \min_{T \in \overline{\mathcal{A}_2}} -U_2(\sigma^1, T)$, which implies that $\max_{\sigma^1 \in \Delta(\overline{\mathcal{A}_1})} \min_{T \in \mathcal{A}_2} -U_2(\sigma^1, T) = \max_{\sigma^1 \in \Delta(\overline{\mathcal{A}_1})} \min_{T \in \overline{\mathcal{A}_2}} -U_2(\sigma^1, T)$. Furthermore, $\forall (\sigma^1, T) \in \Delta(\overline{\mathcal{A}_1}) \times \overline{\mathcal{A}_2}, -U_2(\sigma^1, T) \overset{(2.42)}{=} U_1(\sigma^1, T) - b_2$. Thus, the equilibrium inspection strategies are the optimal solutions of $(\overline{\mathrm{LP}_1})$. An analogous proof can be applied to show that the equilibrium attack strategies are the optimal solutions of $(\overline{\mathrm{LP}_2})$.

□

Proof of Proposition 3.

(i) We show the result by contradiction, that is, suppose that $\exists\, (\sigma^{1^*}, \sigma^{2^*}) \in \Sigma$ such

that $\mathcal{V}_{\sigma^{1^*}}$ is not a set cover. For simplicity, we introduce the following notation:

$$\forall e \in \mathcal{E},\ \eta_{\sigma^{1^*}}(e) \coloneqq \mathbb{E}_{\sigma^{1^*}}[\mathrm{F}(S,e)], \tag{2.59}$$

which is the probability with which component e is monitored by σ^{1^*}. Let us sort the components in nondecreasing order of monitoring probability: $\eta_{\sigma^{1^*}}(e_1) \leq \eta_{\sigma^{1^*}}(e_2) \leq \cdots \leq \eta_{\sigma^{1^*}}(e_{|\mathcal{E}|})$. Then, $T' = \{e_1, \ldots, e_{b_2}\}$ is a best response to σ^{1^*} for **P2** (recall that **P2** uses all her resources; see Proposition 2). Let $T^0 = \{e_1, \ldots, e_k\} \in 2^{\mathcal{E}}$ denote the components that are not monitored by any detector positioning $S \in \mathrm{supp}(\sigma^{1^*})$. Then, $\eta_{\sigma^{1^*}}(e_1) = \cdots = \eta_{\sigma^{1^*}}(e_k) = 0$, and **P2**'s equilibrium payoff is:

$$\begin{aligned} U_2(\sigma^{1^*}, T') &\overset{(2.3)}{=} |T'| - \mathbb{E}_{\sigma^{1^*}}[\mathrm{F}(S,T')] \\ &\overset{(2.38),(2.59)}{=} b_2 - \sum_{e \in T'} \eta_{\sigma^{1^*}}(e) = b_2 - \sum_{i=k+1}^{b_2} \eta_{\sigma^{1^*}}(e_i). \end{aligned} \tag{2.60}$$

Thus, **P1**'s equilibrium payoff in the game $\widetilde{\Gamma}$ is $-b_2 + \sum_{i=k+1}^{b_2} \eta_{\sigma^{1^*}}(e_i)$. Now, to show the contradiction, we construct another strategy $\widehat{\sigma}^1$ that will provide a better payoff than σ^{1^*} to **P1**.

– **Case 1:** $k \geq b_2$. Then **P1**'s equilibrium payoff in $\widetilde{\Gamma}$ is $-b_2$ (it corresponds to zero detections). However, she has an incentive to switch her strategy, and by randomizing over the nodes that can monitor the k components in T^0, she will increase her payoff; which is a contradiction.

– **Case 2:** $k < b_2$. Then **P2** will randomize over attack plans that contain T^0.

- **Case 2.1:** $k \geq b_1$. Then **P1**'s equilibrium payoff in $\widetilde{\Gamma}$ is at least equal to $b_1 - b_2$ (since she can monitor b_1 components in T^0 that are always targeted). This implies that **P2**'s equilibrium payoff is at most $b_2 - b_1$. However, thanks to Proposition 1, we know that **P2**'s equilibrium payoff is larger than or equal to $b_2 - \frac{b_1 b_2}{m^*} > b_2 - b_1$ (since $b_2 < m^*$). Therefore there is a contradiction.

- **Case 2.2:** $k < b_1$. Then, the idea is to construct another strategy that positions k detectors to monitor the components in T^0 (that were previously unmonitored), and that randomizes the positioning of the remaining $b_1 - k$ detectors over the node basis of σ^{1^*}.

For now, assume that **P1** has $b_1 - k$ detectors. For any detector positioning $S \in \text{supp}(\sigma^{1^*})$ (viewed as a set of nodes), we consider $\sigma^1(S, b_1 - k)$ defined in (2.45) (in this case, we randomize the placement of $b_1 - k$ detectors over the set S of size b_1). Recall that $\text{supp}(\sigma^1(S, b_1 - k)) = \{S^1, \dots, S^{b_1}\}$, and that $\forall l \in [\![1, b_1]\!],\ \sigma^1(S, b_1 - k)_{S^l} = \frac{1}{b_1}$. Now, let us construct the following inspection strategy:

$$\sigma^{1'} = \sum_{S \in \text{supp}(\sigma^{1^*})} \sigma^{1^*}_S \sigma^1(S, b_1 - k). \tag{2.61}$$

Then, $\text{supp}(\sigma^{1'}) = \cup_{S \in \text{supp}(\sigma^{1^*})} \{S^1, \dots, S^{b_1}\}$. Notice that it is indeed a probability distribution:

$$\begin{aligned}\sum_{S' \in \mathcal{A}_1} \sigma^{1'}_{S'} &\overset{(2.61)}{=} \sum_{S' \in \mathcal{A}_1} \sum_{S \in \text{supp}(\sigma^{1^*})} \sigma^{1^*}_S \sigma^1(S, b_1 - k)_{S'} \\ &= \sum_{S \in \text{supp}(\sigma^{1^*})} \sigma^{1^*}_S \sum_{S' \in \mathcal{A}_1} \sigma^1(S, b_1 - k)_{S'} = \sum_{S \in \text{supp}(\sigma^{1^*})} \sigma^{1^*}_S = 1,\end{aligned}$$

where we first used the fact that $\forall S \in \text{supp}(\sigma^{1^*}),\ \sigma^1(S, b_1 - k)$ is a probability distribution, and then that σ^{1^*} is a probability distribution.

Thus, $\sigma^{1'}$ is a probability distribution that randomizes over detector positionings of size $b_1 - k$. Then, $\forall S \in \text{supp}(\sigma^{1'})$, we augment S by placing k additional detectors to monitor the subset of components T^0 that was previously unmonitored and that is always targeted in equilibrium by **P2**. We denote $\{i_1, \dots, i_k\}$ the placement of such additional detectors, and we denote $\widehat{S} = S \cup \{i_1, \dots, i_k\},\ \forall S \in \text{supp}(\sigma^{1'})$ the augmented detector positioning. Then, we consider the probability distribution $\widehat{\sigma}^1$ with support equal to

$\cup_{S\in\text{supp}(\sigma^{1^*})}\{\widehat{S}^1,\ldots,\widehat{S}^{b_1}\}$ and such that:

$$\forall S\in\text{supp}(\sigma^{1'}),\ \sigma^{1'}_S=\widehat{\sigma}^1_{\widehat{S}}, \tag{2.62}$$

i.e., $\widehat{\sigma}^1$ is the same probability distribution as $\sigma^{1'}$ except that it randomizes over the augmented detector positionings present in the support of $\sigma^{1'}$.

Then, we can derive the following calculations which combine the previous construction of $\widehat{\sigma}^1$ with a property of the detection function derived in (2.51), and which will lead to a contradiction. $\forall T\in\mathcal{A}_2\mid T^0\subset T$ and $|T|=b_2$:

$$\begin{aligned}
\mathbb{E}_{\widehat{\sigma}^1}[\text{F}(S,T)] &\overset{(2.36)}{=} \mathbb{E}_{\widehat{\sigma}^1}[\underbrace{\text{F}(S,T^0)}_{=k}]+\mathbb{E}_{\widehat{\sigma}^1}[\text{F}(S,T\backslash T^0)]\\
&= k+\sum_{S\in\text{supp}(\sigma^{1^*})}\sum_{l=1}^{b_1}\widehat{\sigma}^1_{\widehat{S}^l}\,\text{F}(\widehat{S}^l,T\backslash T^0)\\
&\overset{(2.35),(2.62)}{\geq} k+\sum_{S\in\text{supp}(\sigma^{1^*})}\sum_{l=1}^{b_1}\sigma^{1'}_{S^l}\,\text{F}(S^l,T\backslash T^0)\\
&\overset{(2.45),(2.61)}{=} k+\sum_{S\in\text{supp}(\sigma^{1^*})}\sum_{l=1}^{b_1}\frac{1}{b_1}\sigma^{1^*}_S\,\text{F}(S^l,T\backslash T^0)\\
&\overset{(2.51)}{\geq} k+\sum_{S\in\text{supp}(\sigma^{1^*})}\frac{b_1-k}{b_1}\sigma^{1^*}_S\,\text{F}(S,T\backslash T^0)\\
&\overset{(2.38),(2.59)}{=} k+\underbrace{\frac{b_1-k}{b_1}}_{>0}\sum_{e\in T\backslash T^0}\eta_{\sigma^{1^*}}(e)\\
&\geq k+\frac{b_1-k}{b_1}\sum_{i=k+1}^{b_2}\eta_{\sigma^{1^*}}(e_i)\\
&= \sum_{i=k+1}^{b_2}\eta_{\sigma^{1^*}}(e_i)+k\left(1-\frac{1}{b_1}\sum_{i=k+1}^{b_2}\eta_{\sigma^{1^*}}(e_i)\right).
\end{aligned}\tag{2.63}$$

From Proposition 1, we know that the equilibrium payoff of **P2** is at least

$b_2 - \frac{b_1 b_2}{m^*}$. Therefore:

$$U_2(\sigma^{1^*}, \sigma^{2^*}) \overset{(2.60)}{=} b_2 - \sum_{i=k+1}^{b_2} \eta_{\sigma^{1^*}}(e_i) \geq b_2 - \frac{b_1 b_2}{m^*}$$
$$\iff \frac{1}{b_1} \sum_{i=k+1}^{b_2} \eta_{\sigma^{1^*}}(e_i) \leq \frac{b_2}{m^*} < 1,$$

since $b_2 < m^*$. Then, by combining the previous inequality with (2.63), we obtain:

$$\forall T \in \mathcal{A}_2 \mid T^0 \subset T \text{ and } |T| = b_2,\ -U_2(\widehat{\sigma}^1, T) \overset{(2.3),(2.63)}{>} -b_2 + \sum_{i=k+1}^{b_2} \eta_{\sigma^{1^*}}(e_i)$$
$$\overset{(2.60)}{=} -U_2(\sigma^{1^*}, \sigma^{2^*}).$$

Since each attack plan in the support of an equilibrium strategy uses all the resources (Proposition 2), and must contain T^0 (beginning of Case 2), then: $-U_2(\widehat{\sigma}^1, \sigma^{2^*}) = \mathbb{E}_{\sigma^{2^*}}[-U_2(\widehat{\sigma}^1, T)] > -U_2(\sigma^{1^*}, \sigma^{2^*})$, which violates the equilibrium condition (2.4) in the strategic equivalent game $\widetilde{\Gamma}$.

Therefore, $\forall (\sigma^{1^*}, \sigma^{2^*}) \in \Sigma,\ \mathcal{V}_{\sigma^{1^*}}$ is a set cover.

(ii) From Proposition 3 and the fact that $b_1 < n^*$, **P1** must randomize her detector positionings in equilibrium so the node basis is a set cover. Now, assume that there exists a NE $(\sigma^{1^*}, T) \in \Sigma$ such that **P2** chooses a pure strategy T (of size b_2 from Proposition 2).

– If $b_1 \geq b_2$, then **P1** can detect all the attacks in T by placing b_2 detectors at the nodes that can monitor the components of T, and **P2**'s equilibrium payoff would be 0. Again, since **P2**'s payoff is identical for any NE, then $U_2(\sigma^{1^*}, T) = 0$. However, we showed in the proof of Proposition 2 that there exists a component outside of T that is not monitored with positive probability by σ^{1^*}. Therefore, **P2** can increase her payoff by targeting that component, thus leading to a contradiction.

– If $b_1 < b_2$, then **P1** can detect at least b_1 attacks in T by placing detectors on b_1 nodes that can collectively monitor b_1 components of T. The resulting payoff for **P1** in the game $\widetilde{\Gamma}$ is at least $b_1 - b_2$. However, from Proposition 1, we know that **P2**'s equilibrium payoff is at least $\max\{0, b_2(1-\frac{b_1}{m^*})\} \geq b_2(1-\frac{b_1}{m^*}) > b_2 - b_1$ (since $b_2 < m^*$). Therefore, **P1**'s equilibrium payoff in $\widetilde{\Gamma}$ is strictly upper bounded by $b_1 - b_2$, thus leading to a contradiction.

Therefore, in equilibrium, both players must randomize their actions.

□

Proof of Theorem 1.

(i) Since **P2**'s expected payoff in the game Γ is also her expected payoff in $\widetilde{\Gamma}$, we know that **P2**'s equilibrium payoff is constant. From Proposition 1, we can directly obtain that $\forall(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma$:

$$\max\left\{0, b_2\left(1 - \frac{b_1}{m^*}\right)\right\} \leq U_2(\sigma^{1^*}, \sigma^{2^*}) \leq b_2\left(1 - \frac{b_1}{n^*}\right). \tag{2.64}$$

By combining (2.42) and Proposition 2, we deduce that **P1**'s payoff in equilibrium of Γ is also constant, and can be bounded as follows:

$$\forall(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma,\ \frac{b_1 b_2}{n^*} \leq U_1(\sigma^{1^*}, \sigma^{2^*}) \leq \min\left\{\frac{b_1 b_2}{m^*}, b_2\right\}. \tag{2.65}$$

(ii) Again, thanks to Proposition 2, we have:

$$\forall\sigma^* \in \Sigma,\ r(\sigma^*) \overset{(2.8)}{=} \mathbb{E}_{\sigma^*}\left[\frac{\mathrm{F}(S,T)}{|T|}\right] = \frac{1}{b_2}\mathbb{E}_{\sigma^*}[\mathrm{F}(S,T)] \overset{(2.2)}{=} \frac{1}{b_2}U_1(\sigma^{1^*}, \sigma^{2^*}).$$

Therefore, from (2.65), we obtain that the expected detection rate in equilibrium is constant and bounded as follows:

$$\forall\sigma^* \in \Sigma,\ \frac{b_1}{n^*} \leq r(\sigma^*) \leq \min\left\{\frac{b_1}{m^*}, 1\right\}.$$

□

Proof of Theorem 2.

(i.a) Let $S^{min} \in \mathcal{S}$ be an MSC and $T^{max} \in \mathcal{M}$ be an MSP. Then, let us show that $(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2))$ is an $\epsilon-$NE where $\epsilon = b_1 b_2 \left(\frac{1}{\max\{b_1, m^*\}} - \frac{1}{n^*}\right)$. First, note that $-\epsilon = \max\left\{0, b_2\left(1 - \frac{b_1}{m^*}\right)\right\} + b_2\left(\frac{b_1}{n^*} - 1\right)$. Then, we have $\forall \sigma^1 \in \Delta(\mathcal{A}_1)$:

$$\begin{aligned}
&- U_2(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2)) \geq \min_{\sigma^2 \in \Delta(\mathcal{A}_2)} -U_2(\sigma^1(S^{min}, b_1), \sigma^2) \\
&\overset{\text{Prop. 1}}{=} b_2\left(\frac{b_1}{n^*} - 1\right) = -\max\left\{0, b_2\left(1 - \frac{b_1}{m^*}\right)\right\} - \epsilon \\
&\overset{\text{Prop. 1}}{=} -\min_{\sigma^{1'} \in \Delta(\mathcal{A}_1)} U_2(\sigma^{1'}, \sigma^2(T^{max}, b_2)) - \epsilon \\
&\geq -U_2(\sigma^1, \sigma^2(T^{max}, b_2)) - \epsilon. \qquad (2.66)
\end{aligned}$$

Therefore, $\forall \sigma^1 \in \Delta(\mathcal{A}_1)$:

$$U_1(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2)) - U_1(\sigma^1, \sigma^2(T^{max}, b_2)) \overset{(2.66),(2.42)}{\geq} -\epsilon.$$

Analogous calculations show that $\forall \sigma^2 \in \Delta(\mathcal{A}_2)$:

$$U_2(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2)) \geq U_2(\sigma^1(S^{min}, b_1), \sigma^2) - \epsilon.$$

Therefore, we conclude that $(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2)) \in \Sigma_\epsilon(b_1, b_2)$.

(i.b) Again, from Proposition 1, we deduce that:

$$\max\left\{0, \left(1 - \frac{b_1}{m^*}\right) b_2\right\} \leq U_2(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2)) \leq b_2\left(1 - \frac{b_1}{n^*}\right).$$

By combining it with (2.64), we obtain:

$$\begin{aligned}
\forall (\sigma^{1^*}, \sigma^{2^*}) \in \Sigma,\ &|U_2(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2)) - U_2(\sigma^{1^*}, \sigma^{2^*})| \\
&\leq b_2\left(1 - \frac{b_1}{n^*}\right) - \max\left\{0, \left(1 - \frac{b_1}{m^*}\right) b_2\right\} = \epsilon.
\end{aligned}$$

Furthermore, from (2.42), (2.18), and (2.44), we also deduce that:

$$\begin{aligned}\forall(\sigma^{1^*},\sigma^{2^*})\in\Sigma,\ &|U_1(\sigma^1(S^{min},b_1),\sigma^2(T^{max},b_2))-U_1(\sigma^{1^*},\sigma^{2^*})|\\ =&|U_2(\sigma^1(S^{min},b_1),\sigma^2(T^{max},b_2))-U_2(\sigma^{1^*},\sigma^{2^*})|\leq\epsilon.\end{aligned}$$

(ii) Consider an MSC $S^{min}\in\mathcal{S}$. Then we have:

$$\begin{aligned}\forall T\in\mathcal{A}_2,\ \frac{U_1(\sigma^1(S^{min},b_1),T)}{|T|}&\overset{(2.42)}{=}\frac{-U_2(\sigma^1(S^{min},b_1),T)}{|T|}+\frac{|T|}{|T|}\\ &\overset{(2.54)}{\geq}\frac{b_1}{n^*}.\end{aligned}\tag{2.67}$$

Thus, by linearity of the expectation, we obtain:

$$\forall\sigma^2\in\Delta(\mathcal{A}_2),\ r(\sigma^1(S^{min},b_1),\sigma^2)\overset{(2.2),(2.8)}{=}\mathbb{E}_{\sigma^2}\left[\frac{U_1(\sigma^1(S^{min},b_1),T)}{|T|}\right]\overset{(2.67)}{\geq}\frac{b_1}{n^*}.$$

Therefore, $\min_{\sigma^2\in\Delta(\mathcal{A}_2)}r(\sigma^1(S^{min},b_1),\sigma^2)\geq\frac{b_1}{n^*}$. Now, consider $i'\in S^{min}$. Recall from (2.52) that $\exists\, e'\in\mathcal{E}\mid \mathrm{F}(i',e')=1$ and $\mathrm{F}(i,e')=0,\ \forall i\in S^{min}\backslash\{i'\}$. Then, it is easy to see that:

$$r(\sigma^1(S^{min},b_1),e')\overset{(2.8),(2.32)}{=}\rho_{\sigma^1(S^{min},b_1)}(i')\overset{(2.47)}{=}\frac{b_1}{n^*}.$$

Therefore, $\min_{\sigma^2\in\Delta(\mathcal{A}_2)}r(\sigma^1(S^{min},b_1),\sigma^2)=\frac{b_1}{n^*}$.

Finally, from Theorem 1, we have $\forall(\sigma^{1^*},\sigma^{2^*})\in\Sigma,\ r(\sigma^{1^*},\sigma^{2^*})\leq\frac{b_1}{\max\{b_1,m^*\}}$, and we can deduce that:

$$\frac{\max\{b_1,m^*\}}{n^*}r(\sigma^{1^*},\sigma^{2^*})\leq\frac{b_1}{n^*}=\min_{\sigma^2\in\Delta(\mathcal{A}_2)}r(\sigma^1(S^{min},b_1),\sigma^2).$$

□

Proof of Corollary 1. By rewriting Theorem 1 when $n^* = m^*$, we obtain $\forall(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma(b_1, b_2)$:

$$\frac{b_1 b_2}{n^*} \leq U_1(\sigma^{1^*}, \sigma^{2^*}) \leq \min\left\{\frac{b_1 b_2}{m^*}, b_2\right\} = \min\left\{\frac{b_1 b_2}{n^*}, b_2\right\} = \frac{b_1 b_2}{n^*},$$
$$b_2\left(1 - \frac{b_1}{n^*}\right) = \max\left\{0, b_2\left(1 - \frac{b_1}{m^*}\right)\right\} \leq U_2(\sigma^{1^*}, \sigma^{2^*}) \leq b_2\left(1 - \frac{b_1}{n^*}\right),$$

since $b_1 < n^*$.

Similarly, for the expected detection rate in equilibrium, we obtain:

$$\forall \sigma^* \in \Sigma(b_1, b_2),\ \frac{b_1}{n^*} \leq r(\sigma^*) \leq \min\left\{\frac{b_1}{m^*}, 1\right\} = \min\left\{\frac{b_1}{n^*}, 1\right\} = \frac{b_1}{n^*}.$$

□

Lemma 7. *For any MSC $S^{min} \in \mathcal{S}$ and any MSP $T^{max} \in \mathcal{M}$ such that $n^* = m^*$, each component in T^{max} is monitored from exactly one node in S^{min}, and each node in S^{min} monitors exactly one component in T^{max}.*

Proof of Lemma 7. Consider an MSC $S^{min} \in \mathcal{S}$ and an MSP $T^{max} \in \mathcal{M}$. Since T^{max} is an MSP, each node in S^{min} monitors at most one component in T^{max}. Now, assume that at least one node in S^{min} does not monitor any component in T^{max}. Since S^{min} is an MSC, then the n^* components in T^{max} are monitored from at most $n^* - 1$ nodes. From Dirichlet's principle, there exists a node in S^{min} that monitors at least two components in T^{max}, which is a contradiction. Therefore, each node in S^{min} monitors exactly one component in T^{max}.

Thus, we can define a mapping $\psi : S^{min} \longrightarrow T^{max}$ such that $\forall i \in S^{min},\ \psi(i)$ is the component in T^{max} that is monitored from node i. Now, since S^{min} is an MSC, for every component $e \in T^{max},\ \exists\, i \in S^{min}$ such that e is monitored from i. Therefore, ψ is surjective which is equivalent to ψ being injective since its domain and codomain have the same number of elements. Therefore, each component in T^{max} is monitored from exactly one node in S^{min}. □

Proof of Proposition 4. For simplicity, given an optimization problem $(\mathcal{Q})$, we denote $z^*_{(\mathcal{Q})}$ its optimal value. Let $S^{min} \in \mathcal{S}$ be an MSC and $T^{max} \in \mathcal{M}$ be an MSP, and assume that they are of same size. Recall that from Proposition 1, we have $z^*_{(\mathrm{LP}_{S^{min}})} \leq z^*_{(\mathrm{LP}_1)} = -z^*_{(\mathrm{LP}_2)} \leq -z^*_{(\mathrm{LP}_{T^{max}})}$. Since $n^* = m^*$ (and $b_1 < n^*$), then we also have:

$$z^*_{(\mathrm{LP}_{S^{min}})} = b_2 \left(\frac{b_1}{n^*} - 1 \right) = -\max \left\{ 0, b_2 \left(1 - \frac{b_1}{m^*} \right) \right\} = -z^*_{(\mathrm{LP}_{T^{max}})}.$$

Therefore, $z^*_{(\mathrm{LP}_{S^{min}})} = z^*_{(\mathrm{LP}_1)}$ and $z^*_{(\mathrm{LP}_{T^{max}})} = z^*_{(\mathrm{LP}_2)}$. Since $(\mathrm{LP}_{S^{min}})$ and $(\mathrm{LP}_{T^{max}})$ are restrictions of (LP_1) and (LP_2) respectively, then any inspection strategy σ^{1^*} (resp. attack strategy σ^{2^*}) that is optimal for $(\mathrm{LP}_{S^{min}})$ (resp. $(\mathrm{LP}_{T^{max}})$) is optimal for (LP_1) (resp. (LP_2)). Thus, any strategy profile $(\sigma^{1^*}, \sigma^{2^*})$ such that σ^{1^*} and σ^{2^*} are optimal solutions of $(\mathrm{LP}_{S^{min}})$ and $(\mathrm{LP}_{T^{max}})$ respectively is a NE.

To show that an inspection strategy σ^{1^*} (whose node basis is S^{min}) is an optimal solution of $(\mathrm{LP}_{S^{min}})$, it is sufficient to show that $\min_{\sigma^2 \in \Delta(\mathcal{A}_2)} -U_2(\sigma^{1^*}, \sigma^2) \geq b_2 \left(\frac{b_1}{n^*} - 1 \right) = z^*_{(\mathrm{LP}_{S^{min}})}$. By applying (2.55) for S^{min} (which is a minimal set cover), we obtain that $\min_{\sigma^2 \in \Delta(\mathcal{A}_2)} -U_2(\sigma^1(S^{min}, b_1), \sigma^2) \geq b_2 \left(\frac{b_1}{n^*} - 1 \right)$. However, recall that to show this inequality, the only property from $\sigma^1(S^{min}, b_1)$ that we used was that its node basis is S^{min} and that $\forall i \in S^{min}$, $\rho_{\sigma^1(S^{min}, b_1)}(i) = \frac{b_1}{n^*}$. Therefore, any inspection strategy that satisfies the same conditions also satisfies the same inequality and is an optimal solution of $(\mathrm{LP}_{S^{min}})$.

Similarly, we can easily deduce from (2.57) that any attack strategy σ^{2^*} whose component basis is T^{max} and which satisfies $\forall e \in T^{max}$, $\rho_{\sigma^{2^*}}(e) = \frac{b_2}{n^*}$ also satisfies the inequality $\min_{\sigma^1 \in \Delta(\mathcal{A}_1)} U_2(\sigma^1, \sigma^{2^*}) \geq b_2 \left(1 - \frac{b_1}{n^*} \right)$ and is an optimal solution of $(\mathrm{LP}_{T^{max}})$.

Thus, any strategy profile $(\sigma^{1^*}, \sigma^{2^*})$ whose node basis is S^{min}, whose component basis is T^{max}, and that satisfies $\rho_{\sigma^{1^*}}(i) = \frac{b_1}{n^*}, \forall i \in S^{min}$, and $\rho_{\sigma^{2^*}}(e) = \frac{b_2}{n^*}$, $\forall e \in T^{max}$, is a NE; it is a sufficient condition.

Now, let us show by contradiction that this is also a necessary condition. Consider a NE $(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma$ whose node basis is an MSC $S^{min} = \{i_1, \ldots, i_{n^*}\} \in \mathcal{S}$, and assume

that the inspection probability is not identical among the nodes in S^{min}. Without loss of generality (by reordering the indices), assume that $\rho_{\sigma^{1^*}}(i_1) < \rho_{\sigma^{1^*}}(i_{b_2+1})$.

Consider an MSP $T^{max} = \{e_1, \ldots, e_{n^*}\} \in \mathcal{M}$. Thanks to Lemma 7, and without loss of generality, we can rearrange the indices such that $\forall k \in [\![1, n^*]\!]$, e_k is only monitored from node i_k in S^{min}. Now consider $\sigma^2(T^{max}, b_2)$ defined in Lemma 6. Since $\sigma^2(T^{max}, b_2)$ satisfies the above-mentioned sufficient conditions, i.e., its component basis is T^{max} and each component of T^{max} is targeted with probability $\frac{b_2}{n^*}$, then $\sigma^2(T^{max}, b_2)$ is an optimal solution of ($\mathrm{LP}_{T^{max}}$). This implies that $(\sigma^{1^*}, \sigma^2(T^{max}, b_2))$ is a NE. Furthermore, the support of $\sigma^2(T^{max}, b_2)$ contains $T^1 = \{e_1\} \cup \{e_2, \ldots, e_{b_2}\}$ and $T^2 = \{e_{b_2+1}\} \cup \{e_2, \ldots, e_{b_2}\}$ (which are different since $b_2 < m^* = n^*$). Therefore, T^1 and T^2 should give the same payoff to **P2**. However, we have the following contradiction:

$$\begin{aligned} U_2(\sigma^{1^*}, T^1) - U_2(\sigma^{1^*}, T^2) &\overset{(2.3),(2.36)}{=} \mathbb{E}_{\sigma^{1^*}}[\mathrm{F}(S, e_{b_2+1})] - \mathbb{E}_{\sigma^{1^*}}[\mathrm{F}(S, e_1)] \\ &= \mathbb{E}_{\sigma^{1^*}}[\mathbb{1}_{\{i_{b_2+1} \in S\}}] - \mathbb{E}_{\sigma^{1^*}}[\mathbb{1}_{\{i_1 \in S\}}] \\ &\overset{(2.32)}{=} \rho_{\sigma^{1^*}}(i_{b_2+1}) - \rho_{\sigma^{1^*}}(i_1) > 0. \end{aligned} \tag{2.68}$$

Note that in (2.68), we used the fact that the node basis of σ^{1^*} is S^{min} and that e_1 (resp. e_{b_2+1}) is only monitored from i_1 (resp. i_{b_2+1}) in S^{min}.

Thus, the inspection probability is necessarily identical among the nodes of S^{min}: $\exists\, \gamma \in \mathbb{R} \mid \forall i \in S^{min},\ \rho_{\sigma^{1^*}}(i) \overset{(2.32)}{=} \sum_{\{S \in \mathcal{A}_1 \,|\, i \in S\}} \sigma_S^{1^*} = \gamma$. By summing over the nodes of S^{min}, and by combining Proposition 2 with the fact that the node basis of σ^{1^*} is S^{min}, we obtain:

$$n^*\gamma = \sum_{i \in S^{min}} \sum_{\{S \in \mathcal{A}_1 \,|\, i \in S\}} \sigma_S^{1^*} = \sum_{S \in \mathcal{A}_1} \sigma_S^{1^*} \sum_{i \in S^{min}} \mathbb{1}_{\{i \in S\}} \overset{(2.17)}{=} b_1 \sum_{S \in \mathcal{A}_1} \sigma_S^{1^*} = b_1.$$

Therefore, $\gamma = \frac{b_1}{n^*}$, meaning that in any NE $(\sigma^{1^*}, \sigma^{2^*})$ whose node basis is an MSC, the inspection probability must be equal to $\frac{b_1}{n^*}$ for all the nodes of the MSC, which proves the necessary condition on the inspection strategy.

Analogously, we can prove that in any NE $(\sigma^{1^*}, \sigma^{2^*})$ whose component basis is an

MSP, the attack probability must be equal to $\frac{b_2}{n^*}$ for all the components of the MSP.

□

Proof of Proposition 5. Let $\sigma^* = (\sigma^{1^*}, \sigma^{2^*}) \in \Sigma$, and assume that $n^* = m^*$. Consider an MSC $S^{min} \in \mathcal{S}$, an MSP $T^{max} \in \mathcal{M}$, and $(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2))$ constructed in Lemma 6.

(i) From Lemma 4, we know that the NE of Γ are interchangeable. Proposition 4 implies that $(\sigma^1(S^{min}, b_1), \sigma^2(T^{max}, b_2))$ defined in (2.45)-(2.46) is a NE. Therefore, $(\sigma^{1^*}, \sigma^2(T^{max}, b_2))$ is also a NE, and we obtain:

$$\begin{aligned}\frac{b_1 b_2}{n^*} &\overset{(2.19)}{=} U_1(\sigma^{1^*}, \sigma^2(T^{max}, b_2)) \overset{(2.2),(2.46)}{=} \mathbb{E}_{\sigma^{1^*}}[\sum_{l=1}^{n^*} \frac{1}{n^*} \mathrm{F}(S, T^l)] \\ &\overset{(2.38)}{=} \frac{1}{n^*}\mathbb{E}_{\sigma^{1^*}}[\sum_{e\in\mathcal{E}} \mathrm{F}(S,e) \sum_{l=1}^{n^*} \mathbb{1}_{\{e\in T^l\}}] \overset{(2.50)}{=} \frac{1}{n^*}\mathbb{E}_{\sigma^{1^*}}[\sum_{e\in T^{max}} \mathrm{F}(S,e) b_2] \\ &\overset{(2.38)}{=} \frac{b_2}{n^*}\mathbb{E}_{\sigma^{1^*}}[\mathrm{F}(S, T^{max})].\end{aligned}$$

Therefore, $\mathbb{E}_{\sigma^{1^*}}[\mathrm{F}(S, T^{max})] = b_1$, from which we deduce that:

$$b_1 = \mathbb{E}_{\sigma^{1^*}}[\mathrm{F}(S, T^{max})] \overset{(2.38),(2.37)}{\leq} \mathbb{E}_{\sigma^{1^*}}[\sum_{i\in S} \mathrm{F}(i, T^{max})] \overset{(2.12)}{\leq} \mathbb{E}_{\sigma^{1^*}}[|S|] \overset{(2.17)}{=} b_1.$$

Then, all the previous inequalities become equalities. The first one implies that $\forall S \in \mathrm{supp}(\sigma^{1^*}),\ \forall e \in T^{max},\ \mathrm{F}(S,e) = \sum_{i\in S} \mathrm{F}(i,e)$.

The second induced equality implies that $\forall i \in \mathcal{V}_{\sigma^{1^*}},\ \mathrm{F}(i, T^{max}) = 1$.

(ii) Similarly, by interchangeability of NE, $(\sigma^1(S^{min}, b_1), \sigma^{2^*}) \in \Sigma$. Then:

$$\frac{b_1 b_2}{n^*} \overset{(2.19)}{=} U_1(\sigma^1(S^{min}, b_1), \sigma^{2^*}) \overset{(2.2),(2.38),(2.45)}{=} \frac{1}{n^*}\mathbb{E}_{\sigma^{2^*}}[\sum_{e\in T} \sum_{k=1}^{n^*} \mathrm{F}(S^k, e)]. \quad (2.69)$$

Since $S^{min} \in \mathcal{S}$, then $\forall e \in \mathcal{E},\ \exists\, i_e \in S^{min} \mid \mathrm{F}(i_e, e) = 1$. Therefore:

$$\forall e \in \mathcal{E},\ \sum_{k=1}^{n^*} \mathrm{F}(S^k, e) = \sum_{\{k \in [\![1,n^*]\!] \,|\, i_e \in S^k\}} 1 + \sum_{\{k \in [\![1,n^*]\!] \,|\, i_e \notin S^k\}} \underbrace{\mathrm{F}(S^k, e)}_{\geq 0}$$
$$\geq |\{k \in [\![1, n^*]\!] \,|\, i_e \in S^k\}| \overset{(2.49)}{=} b_1. \tag{2.70}$$

Thus, we obtain:

$$\frac{b_1 b_2}{n^*} \overset{(2.69),(2.70)}{\geq} \frac{1}{n^*} \mathbb{E}_{\sigma^{2^*}}[\sum_{e \in T} b_1] = \frac{b_1}{n^*} \mathbb{E}_{\sigma^{2^*}}[|T|] \overset{(2.18)}{=} \frac{b_1}{n^*} b_2.$$

Therefore, we obtain the following property:

$$\forall T \in \mathrm{supp}(\sigma^{2^*}),\ \forall e \in T,\ \forall k \in [\![1, n^*]\!] \,|\, i_e \notin S^k,\ \mathrm{F}(S^k, e) = 0. \tag{2.71}$$

Now, consider $T \in \mathrm{supp}(\sigma^{2^*})$, $e \in T$, and let $i_e \in S^{min}$ be a node that satisfies $\mathrm{F}(i_e, e) = 1$. Consider $i' \in S^{min}$ such that $i' \neq i_e$. Since $b_1 < n^*$, then there exists a detector positioning $S^{k'}$ in the support of $\sigma^1(S^{min}, b_1)$ that satisfies $i' \in S^{k'}$ and $i_e \notin S^{k'}$. From (2.71), we deduce that $0 \leq \mathrm{F}(i', e) \overset{(2.35)}{\leq} \mathrm{F}(S^{k'}, e) \overset{(2.71)}{=} 0$. Therefore, for any $i' \in S^{min}$ such that $i' \neq i_e$, i' does not monitor e, which implies that e is only monitored from i_e in S^{min}. Thus:

$$\forall e \in \mathcal{E}_{\sigma^{2^*}},\ \forall S^{min} \in \mathcal{S},\ \exists\,! \, i \in S^{min} \mid \mathrm{F}(i, e) = 1.$$

□

2.9.3 Proofs of Section 2.4

Proposition 8. *Consider a detection model $\mathcal{G}$ that satisfies $n^* = m^*$, a target detection performance $\alpha \in [0, 1]$, and **P2**'s resources $b_2 < m^*$. Then, for any MSC $S^{min} \in \mathcal{S}$ and any MSP $T^{max} \in \mathcal{M}$, an optimal solution of ($\mathcal{P}$) is given by $\lceil \alpha n^* \rceil$, $(\sigma^1(S^{min}, \lceil \alpha n^* \rceil), \sigma^2(T^{max}, b_2))$.*

Proof of Proposition 8. When $n^* = m^*$, we know from Corollary 1 that $\forall \sigma^* \in \Sigma,\ r(\sigma^*) = \frac{b_1}{n^*}$. Therefore, $(\mathcal{P})$ can be rewritten as follows:

$$\begin{aligned} \underset{b_1,\,\sigma^\dagger}{\text{minimize}} \quad & b_1 \\ \text{subject to} \quad & \frac{b_1}{n^*} \geq \alpha, \\ & \sigma^\dagger \in \Sigma(b_1, b_2), \\ & b_1 \in \mathbb{N}. \end{aligned}$$

Then, the optimal value of $(\mathcal{P})$ in this case is $b_1^\dagger = \lceil \alpha n^* \rceil$.

Now, consider an MSC $S^{min} \in \mathcal{S}$ and an MSP $T^{max} \in \mathcal{M}$. From Lemma 1 and Proposition 4, we deduce that $(\sigma^1(S^{min}, b_1^\dagger), \sigma^2(T^{max}, b_2)) \in \Sigma(b_1^\dagger, b_2)$, i.e., is a NE of the game induced by $b_1^\dagger$ and b_2. Therefore, $\lceil \alpha n^* \rceil, (\sigma^1(S^{min}, b_1^\dagger), \sigma^2(T^{max}, b_2))$ is an optimal solution of $(\mathcal{P})$. □

Proof of Proposition 6. Recall that in the general case $m^* \leq n^*$, we admit a relaxation of $(\mathcal{P})$ and consider instead the following mathematical program with equilibrium constraints:

$$\begin{aligned} (\mathcal{P}_\epsilon): \quad \underset{b_1,\,\sigma^\dagger}{\text{minimize}} \quad & b_1 \\ \text{subject to} \quad & r(\sigma^*) \geq \alpha, \qquad \forall \sigma^* \in \Sigma(b_1, b_2) \\ & \sigma^\dagger \in \Sigma_\epsilon(b_1, b_2) \\ & b_1 \in \mathbb{N}, \end{aligned} \tag{2.72}$$

for some $\epsilon \geq 0$.

In this case, we know from the lower bound in Theorem 1 that $\forall b_1 < n^*, \forall \sigma^* \in \Sigma(b_1, b_2), \quad \frac{b_1}{n^*} \leq r(\sigma^*)$. Therefore, constraints (2.72) are satisfied if $b_1 \geq b_1' \coloneqq \lceil \alpha n^* \rceil$. Now, consider an MSC $S^{min} \in \mathcal{S}$ and an MSP $T^{max} \in \mathcal{M}$. We know from Theorem 2 that $(\sigma^1(S^{min}, b_1'), \sigma^2(T^{max}, b_2)) \in \Sigma_\epsilon(b_1', b_2)$, where $\epsilon = b_1' b_2 \left(\frac{1}{\max\{b_1', m^*\}} - \frac{1}{n^*} \right)$. Therefore, $b_1', (\sigma^1(S^{min}, b_1'), \sigma^2(T^{max}, b_2))$ is a feasible solution of $(\mathcal{P}_\epsilon)$ (with the same ϵ), and the corresponding objective value is b_1'.

Finally, from the upper bound in Theorem 1, we know that $\forall b_1 < n^*, \forall \sigma^* \in$

$\Sigma(b_1, b_2)$, $r(\sigma^*) \leq \min\left\{\frac{b_1}{m^*}, 1\right\}$. Therefore, constraints (2.72) cannot be satisfied if $b_1 < \lceil \alpha m^* \rceil$. This implies that an optimality gap associated with $b_1', (\sigma^1(S^{min}, b_1'), \sigma^2(T^{max}, b_2))$ is given by $\lceil \alpha n^* \rceil - \lceil \alpha m^* \rceil$. □

2.9.4 Proofs of Section 2.7

Lemma 8. *Given $b_2 < m^*$, let $\rho \in [0,1]^{|\mathcal{E}|}$ that satisfies $\sum_{e\in\mathcal{E}} \rho_e = b_2$. Then, there exists an attack strategy $\sigma^2 \in \Delta(\mathcal{A}_2)$ that satisfies $\forall e \in \mathcal{E},\ \rho_{\sigma^2}(e) = \rho_e$.*

Proof of Lemma 8. Given $b_2 < m^*$, let $\boldsymbol{A}$ be the $|\mathcal{E}| \times \binom{|\mathcal{E}|}{b_2}$ binary matrix whose rows (resp. columns) are indexed by the components (resp. the size-b_2 subsets) of $\mathcal{E}$, and which satisfies $\forall (e, T) \in \mathcal{E} \times \overline{\mathcal{A}_2},\ a_{e,T} = \mathbb{1}_{\{e\in T\}}$. Then, given $\rho \in [0,1]^{|\mathcal{E}|}$ that satisfies $\sum_{e\in\mathcal{E}} \rho_e = b_2$, we must show that the following system of equations has a feasible solution:

$$\begin{aligned} \boldsymbol{A}\sigma^2 &= \rho \\ \mathbf{1}_{|\overline{\mathcal{A}_2}|}^\top \sigma^2 &= 1 \\ \sigma^2 &\geq \mathbf{0}_{|\overline{\mathcal{A}_2}|}. \end{aligned}$$

Since each $T \in \overline{\mathcal{A}_2}$ is of size b_2, it is easy to see that $\frac{1}{b_2}\mathbf{1}_{|\mathcal{E}|}^\top \boldsymbol{A} = \mathbf{1}_{|\overline{\mathcal{A}_2}|}^\top$. Furthermore, since $\frac{1}{b_2}\mathbf{1}_{|\mathcal{E}|}^\top \rho = 1$, it implies that if σ^2 satisfies $\boldsymbol{A}\sigma^2 = \rho$, it also satisfies $\mathbf{1}_{|\overline{\mathcal{A}_2}|}^\top \sigma^2 = 1$. Therefore, we only need to show that there exists $\sigma^2 \geq \mathbf{0}_{|\overline{\mathcal{A}_2}|}$ such that $\boldsymbol{A}\sigma^2 = \rho$. By Farkas' lemma, such a solution exists if and only if there does not exist $w \in \mathbb{R}^{|\mathcal{E}|}$ such that $w^\top \boldsymbol{A} \leq \mathbf{0}_{|\overline{\mathcal{A}_2}|}^\top$ and $w^\top \rho > 0$.

Let $w \in \mathbb{R}^{|\mathcal{E}|}$ that satisfies $w^\top \boldsymbol{A} \leq \mathbf{0}_{|\overline{\mathcal{A}_2}|}^\top$, and let us order the components in $\mathcal{E}$ so that $w_{e_1} \geq \cdots \geq w_{e_{|\mathcal{E}|}}$. For notational simplicity, let $w_k \coloneqq w_{e_k}$ and $\rho_k \coloneqq \rho_{e_k}$, $\forall k \in [\![1, |\mathcal{E}|]\!]$. Note that since $T^1 = \{e_1, \ldots, e_{b_2}\} \in \overline{\mathcal{A}_2}$, we have $\sum_{k=1}^{b_2} w_k = (w^\top \boldsymbol{A})_{T^1} \leq 0$.

Then, we obtain:

$$w^\top \rho = \sum_{k=1}^{|\mathcal{E}|} w_k \rho_k = \underbrace{\sum_{k=1}^{b_2} w_k}_{\leq 0} + \sum_{k=b_2+1}^{|\mathcal{E}|} \underbrace{w_k}_{\leq w_{b_2}} \underbrace{\rho_k}_{\geq 0} - \sum_{k=1}^{b_2} \underbrace{w_k}_{\geq w_{b_2}} \underbrace{(1-\rho_k)}_{\geq 0}$$
$$\leq w_{b_2} \left(\sum_{k=1}^{|\mathcal{E}|} \rho_k - b_2 \right) = 0.$$

Therefore, there does not exist $w \in \mathbb{R}^{|\mathcal{E}|}$ such that $w^\top \boldsymbol{A} \leq \mathbf{0}^\top_{|\overline{\mathcal{A}_2}|}$ and $w^\top \rho > 0$, which, by Farkas' lemma, implies that there exists an attack strategy $\sigma^2 \in \Delta(\mathcal{A}_2)$ such that $\forall e \in \mathcal{E},\ \rho_{\sigma^2}(e) = \rho_e$. □

Proof of Theorem 3. Consider **P1**'s amount of resources b_1. If $b_1 \geq n^*$, then it is easy to see that $\forall b_2 < m^*$, $\forall \sigma^* \in \Sigma(b_1, b_2)$, $r(\sigma^*) = 1$. Henceforth, we assume that $b_1 < n^*$. Recall from Proposition 2 that the NE of Γ can be obtained by solving $(\overline{\mathrm{LP}_1})$ and $(\overline{\mathrm{LP}_2})$.

(i) First, we show that for $b_2 = 1$, there exists an optimal solution of $(\overline{\mathrm{LP}_2})$, $\sigma^{2^*} \in \Delta(\overline{\mathcal{A}_2})$, that satisfies $\forall e \in \mathcal{E},\ \rho_{\sigma^{2^*}}(e) \leq \frac{1}{m^*}$. Since $b_2 = 1$, then $\overline{\mathcal{A}_2} = \mathcal{E}$, and $\forall \sigma^2 \in \Delta(\mathcal{E}),\ \forall e \in \mathcal{E},\ \sigma^2_e = \rho_{\sigma^2}(e)$.

– Consider an optimal solution of $(\overline{\mathrm{LP}_2})$, $\sigma^{2^*} \in \Delta(\mathcal{E})$, and assume on the contrary that $\exists\, e' \in \mathcal{E},\ \exists\, \varepsilon > 0 \mid \rho_{\sigma^{2^*}}(e') = \frac{1}{m^*} + \varepsilon$. Let $S^* \in \arg\max_{S \in \overline{\mathcal{A}_1}} U_1(S, \sigma^{2^*})$. From Proposition 1, we know that:

$$U_1(S^*, \sigma^{2^*}) \overset{(2.42)}{=} -U_2(S^*, \sigma^{2^*}) + 1 \leq -\max\{1 - \frac{b_1}{m^*}, 0\} + 1 \leq \frac{b_1}{m^*}. \tag{2.73}$$

Therefore, we can show that $\exists\, i' \in S^* \mid U_1(S^*, \sigma^{2^*}) - U_1(S^* \backslash \{i'\}, \sigma^{2^*}) \leq \frac{1}{m^*}$. Indeed, if $\forall i \in S^*,\ U_1(S^*, \sigma^{2^*}) - U_1(S^* \backslash \{i\}, \sigma^{2^*}) > \frac{1}{m^*}$, then we obtain the

following contradiction:

$$(b_1-1)U_1(S^*,\sigma^{2^*}) \overset{(2.2),(2.51)}{\leq} \sum_{i\in S^*} U_1(S^*\backslash\{i\},\sigma^{2^*}) < b_1 U_1(S^*,\sigma^{2^*}) - \frac{b_1}{m^*}$$
$$\overset{(2.73)}{\leq} (b_1-1)U_1(S^*,\sigma^{2^*}).$$

– This implies that $e' \in \mathcal{C}_{S^*}$: If $e' \notin \mathcal{C}_{S^*}$ instead, then repositioning the detector on node i' to a node that can monitor e' improves **P1**'s payoff by at least ε and contradicts the definition of S^*:

$$\begin{aligned}
U_1(S^*\backslash\{i'\}\cup\{i^*\},\sigma^{2^*}) &\overset{(2.2)}{=} \sigma_{e'}^{2^*} + \sum_{e\in\mathcal{E}\backslash\{e'\}} \sigma_e^{2^*}\,\mathrm{F}(S^*\backslash\{i'\}\cup\{i^*\},e)\\
&\overset{(2.35)}{\geq} \sigma_{e'}^{2^*} + \sum_{e\in\mathcal{E}} \sigma_e^{2^*}\,\mathrm{F}(S^*\backslash\{i'\},e)\\
&\overset{(2.2)}{=} \varepsilon + \frac{1}{m^*} + U_1(S^*\backslash\{i'\},\sigma^{2^*}) - U_1(S^*,\sigma^{2^*}) + U_1(S^*,\sigma^{2^*})\\
&\geq \varepsilon + U_1(S^*,\sigma^{2^*}) > \max_{S\in\overline{\mathcal{A}_1}} U_1(S,\sigma^{2^*}).
\end{aligned}$$

– Then, we show that at least b_1 components are monitored by S^*. Let $\widehat{\sigma}^2 \in \Delta(\mathcal{E})$ denote the uniform probability over the set of components $\mathcal{E}$, and let $\widehat{S} \in \arg\max_{S\in\overline{\mathcal{A}_1}} U_1(S,\widehat{\sigma}^2)$. Since $b_1 < n^*$, $\exists\,\widehat{e} \in \mathcal{E} \mid \mathrm{F}(\widehat{S},\widehat{e}) = 0$. Then, we obtain:

$$\begin{aligned}
U_1(S^*,\sigma^{2^*}) = \min_{\sigma^2\in\Delta(\mathcal{E})} \max_{S\in\overline{\mathcal{A}_1}} U_1(S,\sigma^2) &\leq \max_{S\in\overline{\mathcal{A}_1}} U_1(S,\widehat{\sigma}^2) = U_1(\widehat{S},\widehat{\sigma}^2)\\
&\overset{(2.2)}{=} \sum_{e\in\mathcal{E}\backslash\{\widehat{e}\}} \widehat{\sigma}_e^2 \underbrace{\mathrm{F}(\widehat{S},e)}_{\leq 1} \leq \sum_{e\in\mathcal{E}} \widehat{\sigma}_e^2 - \widehat{\sigma}_{\widehat{e}}^2 = 1 - \widehat{\sigma}_{\widehat{e}}^2 < 1. \qquad (2.74)
\end{aligned}$$

If we assume that $|\mathcal{C}_{S^*}| < b_1$, then at least one detector in S^* can be removed without changing **P1**'s payoff. Let $i_0 \in S^*$ denote the location of that detector. Now, we can show that $\exists\, e \in \mathcal{E}\backslash\{\mathcal{C}_{S^*}\} \mid \sigma_e^{2^*} > 0$: if on the contrary, we had $\forall e \in \mathcal{E}\backslash\{\mathcal{C}_{S^*}\},\ \sigma_e^{2^*} = 0$, then we would obtain $U_1(S^*,\sigma^{2^*}) = 1$, which contradicts (2.74). Let $e \in \mathcal{E}\backslash\{\mathcal{C}_{S^*}\} \mid \sigma_e^{2^*} > 0$ and let $i \in \mathcal{V} \mid \mathrm{F}(i,e) = 1$. Repositioning the

detector from node i_0 to node i will increase **P1**'s payoff by at least $\sigma_e^{2^*}$, which contradicts the definition of S^*. Thus, $|\mathcal{C}_{S^*}| \geq b_1$.

– Now, we show that we can construct $\sigma^{2'}$ which is the same probability distribution as σ^{2^*} except that it reallocates ε probability from e' to a subset of components T^1 monitored by S^* while ensuring that the attack probability of each component in T^1 is not above $\frac{1}{m^*}$. Let us split $\mathcal{C}_{S^*}$ into $\{e'\}$, $T^1 \coloneqq \{e \in \mathcal{C}_{S^*} \backslash \{e'\} \mid \sigma_e^{2^*} < \frac{1}{m^*}\}$, and $T^2 \coloneqq \{e \in \mathcal{C}_{S^*} \backslash \{e'\} \mid \sigma_e^{2^*} \geq \frac{1}{m^*}\}$. Now, we have:

$$\begin{aligned}\varepsilon &\overset{(2.2)}{=} U_1(S^*, \sigma^{2^*}) - \sum_{e \in T^1 \cup T^2} \sigma_e^{2^*} - \frac{1}{m^*} \overset{(2.73)}{\leq} \frac{b_1 - |T^2| - 1}{m^*} - \sum_{e \in T^1} \sigma_e^{2^*} \\ &\leq \frac{|\mathcal{C}_{S^*}| - |T^2| - 1}{m^*} - \sum_{e \in T^1} \sigma_e^{2^*} = \sum_{e \in T^1} (\frac{1}{m^*} - \sigma_e^{2^*}),\end{aligned}$$

which implies that $T^1 \neq \emptyset$, and that it is possible to allocate ε additional probability to components in T^1 so that the attack probability of each component in T^1 is not above $\frac{1}{m^*}$. Thus, $\sigma^{2'}$ can be constructed. It satisfies $\forall e \in \mathcal{E} \backslash \{T^1 \cup \{e'\}\}$, $\sigma_e^{2'} = \sigma_e^{2^*}$, $\sigma_{e'}^{2'} = \sigma_{e'}^{2^*} - \varepsilon$, and $\sum_{e \in T^1} (\sigma_e^{2'} - \sigma_e^{2^*}) = \varepsilon$.

– Now, consider $S' \in \arg\max_{S \in \overline{\mathcal{A}_1}} U_1(S, \sigma^{2'})$. The goal of this step is to show (by contradiction) that $e' \in \mathcal{C}_{S'}$. First, we derive the following calculations:

$$\begin{aligned}U_1(S', \sigma^{2'}) &\overset{(2.2)}{=} (\sigma_{e'}^{2^*} - \varepsilon)\, \mathrm{F}(S', e') + \sum_{e \in \mathcal{E} \backslash \{T^1 \cup \{e'\}\}} \sigma_e^{2^*}\, \mathrm{F}(S', e) \\ &\quad + \sum_{e \in T^1} \underbrace{(\sigma_e^{2'} - \sigma_e^{2^*})}_{\geq 0} \underbrace{\mathrm{F}(S', e)}_{\leq 1} + \sum_{e \in T^1} \sigma_e^{2^*}\, \mathrm{F}(S', e) \\ &\leq \sum_{e \in \mathcal{E}} \sigma_e^{2^*}\, \mathrm{F}(S', e) + \sum_{e \in T^1} (\sigma_e^{2'} - \sigma_e^{2^*}) - \varepsilon\, \mathrm{F}(S', e') \\ &\overset{(2.2)}{=} U_1(S', \sigma^{2^*}) + \varepsilon(1 - \mathrm{F}(S', e')). \qquad (2.75)\end{aligned}$$

Thus, if $e' \notin \mathcal{C}_{S'}$, then $U_1(S', \sigma^{2'}) \leq U_1(S', \sigma^{2^*}) + \varepsilon$. Since we assumed that each component can be monitored from at least one location (Section 2.2.2), we

deduce that $\exists\, i^* \in \mathcal{V}\backslash S' \mid e' \in \mathcal{C}_{i^*}$. Then, we have:

$$\forall i \in S',\ U_1(S^*, \sigma^{2^*}) \geq U_1(\{i^*\} \cup S'\backslash\{i\}, \sigma^{2^*}) \overset{(2.2),(2.35)}{\geq} \frac{1}{m^*} + \varepsilon + U_1(S'\backslash\{i\}, \sigma^{2^*}). \tag{2.76}$$

Next, we can derive the following calculations:

$$\begin{aligned} U_1(S', \sigma^{2^*}) &\overset{(2.2),(2.51)}{\leq} \frac{1}{b_1 - 1} \sum_{i \in S'} U_1(S'\backslash\{i\}, \sigma^{2^*}) \\ &\overset{(2.76)}{\leq} \frac{1}{b_1 - 1}((b_1 - 1)U_1(S^*, \sigma^{2^*}) + U_1(S^*, \sigma^{2^*}) - \frac{b_1}{m^*} - b_1\varepsilon) \\ &\overset{(2.73)}{\leq} U_1(S^*, \sigma^{2^*}) - \frac{b_1}{b_1 - 1}\varepsilon. \end{aligned} \tag{2.77}$$

Combining everything together, we obtain the following contradiction:

$$\begin{aligned} \max_{S \in \overline{\mathcal{A}_1}} U_1(S, \sigma^{2'}) &\overset{(2.75),(2.77)}{\leq} U_1(S^*, \sigma^{2^*}) - \frac{1}{b_1 - 1}\varepsilon \\ &< U_1(S^*, \sigma^{2^*}) = \min_{\sigma^2 \in \Delta(\mathcal{E})} \max_{S \in \overline{\mathcal{A}_1}} U_1(S, \sigma^2). \end{aligned}$$

– Therefore, we showed that $e' \in \mathcal{C}_{S'}$. This implies that $\varepsilon(1 - \mathrm{F}(S', e')) = 0$, and we obtain:

$$\max_{S \in \overline{\mathcal{A}_1}} U_1(S, \sigma^{2'}) \overset{(2.75)}{\leq} U_1(S', \sigma^{2^*}) \leq \max_{S \in \overline{\mathcal{A}_1}} U_1(S, \sigma^{2^*}) = \min_{\sigma^2 \in \Delta(\mathcal{E})} \max_{S \in \overline{\mathcal{A}_1}} U_1(S, \sigma^2).$$

Thus, $\sigma^{2'}$ is also an optimal solution of $(\overline{\mathrm{LP}_2})$. Therefore, if an optimal solution of $(\overline{\mathrm{LP}_2})$ is such that at least one component is targeted with probability more than $\frac{1}{m^*}$, we can construct another optimal solution of $(\overline{\mathrm{LP}_2})$ with one less component targeted with probability more than $\frac{1}{m^*}$. We can then repeat this process until all attack probabilities are no more than $\frac{1}{m^*}$.

(ii) Given $b_1 < n^*$, let $z^*(b_2)$ denote the optimal value of $(\overline{\mathrm{LP}_2})$ for any $b_2 < m^*$. Now, consider $b_2 < m^*$, and let $\sigma^{2^*} \in \Delta(\mathcal{A}_2)$ be an optimal solution of $(\overline{\mathrm{LP}_2})$. Since $\sum_{e \in \mathcal{E}} \frac{\rho_{\sigma^{2^*}}(e)}{b_2} = 1$, we can construct an attack strategy $\sigma^{2'} \in \Delta(\mathcal{E})$ such

that $\forall e \in \mathcal{E},\ \sigma_e^{2'} = \rho_{\sigma^{2'}}(e) = \frac{\rho_{\sigma^{2^*}}(e)}{b_2}$. Then, the additivity of F gives us:

$$z^*(b_2) \overset{(2.2),(2.33),(2.38)}{=} \max_{S \in \overline{\mathcal{A}_1}} \sum_{e \in \mathcal{E}} \mathrm{F}(S,e)\rho_{\sigma^{2^*}}(e) \overset{(2.2)}{=} b_2 \max_{S \in \overline{\mathcal{A}_1}} U_1(S, \sigma^{2'}) \geq b_2 z^*(1).$$

Now, consider $\widetilde{\sigma}^2 \in \Delta(\mathcal{E})$ which is an optimal solution of $(\overline{\mathrm{LP}_2})$ (where the number of attack resources is 1) with the additional property that $\forall e \in \mathcal{E},\ \rho_{\widetilde{\sigma}^2}(e) \leq \frac{1}{m^*}$. Then, given $b_2 < m^*$, since $\forall e \in \mathcal{E},\ b_2\rho_{\widetilde{\sigma}^2}(e) \leq 1$ and $\sum_{e \in \mathcal{E}} b_2\rho_{\widetilde{\sigma}^2}(e) = b_2$, there exists a probability distribution $\widehat{\sigma}^2 \in \Delta(\mathcal{A}_2)$, that satisfies $\rho_{\widehat{\sigma}^2}(e) = b_2\rho_{\widetilde{\sigma}^2}(e),\ \forall e \in \mathcal{E}$ (Lemma 8). Then, by additivity of F, we obtain:

$$z^*(1) \overset{(2.2)}{=} \max_{S \in \overline{\mathcal{A}_1}} \sum_{e \in \mathcal{E}} \mathrm{F}(S,e)\rho_{\widetilde{\sigma}^2}(e) \overset{(2.2),(2.33),(2.38)}{=} \frac{1}{b_2} \max_{S \in \overline{\mathcal{A}_1}} U_1(S, \widehat{\sigma}^2) \geq \frac{1}{b_2} z^*(b_2).$$

Thus, $\forall b_2 < m^*,\ z^*(b_2) = b_2 z^*(1)$. Therefore, we conclude that:

$$\forall \sigma^* \in \Sigma(b_1, b_2),\ r(\sigma^*) \overset{(2.18)}{=} \frac{U_1(\sigma^*)}{b_2} = \frac{z^*(b_2)}{b_2} = z^*(1) =: r^*_{b_1},$$

which does not depend on b_2.

□

Proof of Proposition 7. Given **P1**'s resources $b_1 < n^*$, let $\sigma^{1^*} \in \Delta(\overline{\mathcal{A}_1})$ be an inspection strategy in equilibrium of the game $\Gamma(b_1, 1)$. From Proposition 2, we know that σ^{1^*} is an optimal solution of $(\overline{\mathrm{LP}_1})$ for $b_2 = 1$. Now, consider $b_2 < m^*$. We can derive the following inequality:

$$\forall T \in \overline{\mathcal{A}_2},\ U_1(\sigma^{1^*}, T) \overset{(2.38)}{=} \sum_{e \in T} U_1(\sigma^{1^*}, e) \geq \sum_{e \in T} \underbrace{\min_{e' \in \mathcal{E}} U_1(\sigma^{1^*}, e')}_{= r^*_{b_1}} = b_2 r^*_{b_1}$$
$$\overset{(2.31)}{=} \max_{\sigma^1 \in \Delta(\overline{\mathcal{A}_1})} \min_{T' \in \overline{\mathcal{A}_2}} U_1(\sigma^1, T').$$

Since this inequality is valid for any $T \in \overline{\mathcal{A}_2}$, we deduce that $\min_{T \in \overline{\mathcal{A}_2}} U_1(\sigma^{1^*}, T) \geq \max_{\sigma^1 \in \Delta(\overline{\mathcal{A}_1})} \min_{T \in \overline{\mathcal{A}_2}} U_1(\sigma^1, T)$. Therefore, σ^{1^*} is an optimal solution of $(\overline{\mathrm{LP}_1})$ (when

the number of attack resources is b_2), and is an inspection strategy in equilibrium of the game $\Gamma(b_1, b_2)$. $\square$

Chapter 3

Strategic Interdiction of Malicious Network Flows

3.1 Introduction

In this chapter, we study the problem of showing the existence of a probability distribution over a partially ordered set (or poset) that satisfies a set of constraints involving marginal probabilities of the poset's elements and maximal chains. This problem is directly motivated by the technical issues arising in the equilibrium analysis of a generic network security game, in which a strategic interdictor seeks to disrupt the flow of a routing entity. In particular, our existence result on posets enables us to show that the equilibrium structure of the game can be described using primal and dual solutions of a minimum cost circulation problem. Furthermore, we show that the set of critical components for our network security game can be characterized using strict complementary slackness in linear programming.

3.1.1 Probability Distributions over Posets

For a given finite nonempty poset, we consider a problem in which each element is associated with a value between 0 and 1; additionally, each maximal chain has a value at most 1. We want to determine if there exists a probability distribution over

the subsets of the poset such that: (i) The probability with which each element of the poset is in a subset is *equal to* its corresponding value; and (ii) the probability with which each maximal chain of the poset intersects with a subset is *as large as* its corresponding value. Solving this problem, denoted $(\mathcal{D})$, is equivalent to resolving the feasibility of a polyhedral set. However, geometric ideas – such as the ones involving the use of Farkas' lemma or Carathéodory's theorem – cannot be applied to solve this problem, because they do not capture the structure of posets. We positively resolve problem $(\mathcal{D})$ under two conditions that are naturally satisfied for our purposes:

1. The value of each maximal chain is no more than the sum of the values of its elements.

2. The values of the maximal chains satisfy a conservation law. Particularly, let C be the union of two intersecting maximal chains. Then, for any decomposition of C into two maximal chains, the sum of the corresponding values is constant.

Under these two conditions, we prove the feasibility of problem $(\mathcal{D})$ (Theorem 4). First, we show that solving $(\mathcal{D})$ is equivalent to proving that the optimal value of an exponential-size linear optimization problem, denoted $(\mathcal{Q})$, is no more than 1 (Proposition 9). Then, to optimally solve $(\mathcal{Q})$, we design a combinatorial algorithm (Algorithm 1) that exploits the relation between the values associated with the poset's elements and maximal chains. In particular, we show that the optimal value of $(\mathcal{Q})$ can be computed in closed form: it is equal to the largest value associated with an element or maximal chain of the poset, which is no more than 1 (Theorem 5). Each iteration of the algorithm involves constructing a subposet, selecting its set of minimal elements, and assigning a specific weight to it. The proof of optimality of the algorithm is carried out in three steps: First, we prove that it is well-defined (Proposition 10). Secondly, we show that it terminates and outputs a feasible solution of $(\mathcal{Q})$ (Proposition 11). Finally, we show that at termination, it assigns a total weight that is exactly equal to the optimal value of $(\mathcal{Q})$ (Proposition 12). Importantly, in the design of the algorithm, we need to ensure that the conservation law satisfied by the values associated with the maximal chains of the poset is preserved after

each iteration. This design feature enables us to obtain a relation between maximal chains after each iteration (Lemma 11), which leads to optimality guarantees of the algorithm.

Next, we show that the feasibility of problem ($\mathcal{D}$) on posets is crucial for the equilibrium analysis of a class of two-player non-cooperative games on flow networks.

3.1.2 Network Security Games

We model a network security game between player 1 (routing entity) that sends its flow through the network while facing heterogeneous path transportation costs; and player 2 (interdictor) who simultaneously chooses an interdiction plan comprised of one or more edges. Player 1 (resp. player 2) seeks to maximize the value of effective (resp. interdicted) flow net the transportation (resp. interdiction) cost. We adopt mixed strategy Nash equilibria as the solution concept of this game.

Our security game is rich and general in that it models heterogeneous costs of transportation and interdiction. It models the strategic situation in which player 1 is an operator who wants to route flow (e.g. water, oil, or gas) through pipelines, while player 2 is an attacker who targets multiple pipes in order to steal or disrupt the flow. An alternative setting is the one where player 1 is a malicious entity composed of routers who carry illegal (or dangerous) goods through a transportation network (i.e., roads, rivers, etc.), and player 2 is a security agency that dispatches interdictors to intercept malicious routers and prevent the illegal goods from crossing the network. In both these settings, mixed strategies can be viewed as the players introducing randomization in implementing their respective actions. For instance, player 1's mixed strategy models a randomized choice of paths for routing its flow of goods through the network, while player 2's mixed strategy indicates a randomized dispatch of interdictors to disrupt or intercept the flow.

The existing literature in network interdiction has dealt with this type of problems in a sequential (Stackelberg) setting (see [10, 12, 94, 114]). Typically, these problems are solved using large-scale integer programming techniques, and are staple for designing system interdiction and defense (see [18, 24, 80, 101, 115]). However, these models

do not capture the situations in which the interdictor is capable of simultaneously interdicting multiple edges, possibly in a randomized manner. Recently, Bertsimas et al. [17] considered a sequential game in which the interdictor first randomly interdicts a fixed number of edges, and then the operator routes a feasible flow in the network. The interdictor's goal is to minimize the largest amount of flow that reaches the destination node. Although this model is equivalent to a simultaneous game, our model is general in that we do not impose any restriction on the number of edges that can be simultaneously interdicted. Additionally, we account for transportation and interdiction costs faced by the players.

Our work is also motivated by previous problems studied in network security games (e.g. [13, 43, 102]). However, the available results in this line of work are for simpler cases, and do not apply to our model. Related to our work are the network security games proposed by Washburn and Wood [112] and Gueye and Marbukh [42]. In [112], the authors consider a simultaneous game where an evader chooses one source-destination path and the interdictor inspects one edge. In this model, the interdictor's (resp. evader's) objective is to maximize (resp. minimize) the probability with which the evader is detected by the interdictor. Gueye and Marbukh [42] model an operator who routes a feasible flow in the network, and an attacker who disrupts one edge. The attacker's (resp. operator's) goal is to maximize (minimize) the amount of lost flow. Additionally, the attacker faces a cost of attack. In contrast, our model allows the interdictor to inspect multiple edges simultaneously, and accounts for the transportation cost faced by the routing entity.

The generality of our model renders known methods for analyzing security games inapplicable to our game. Indeed, prior work has considered solution approaches based on max-flows and min-cuts, and used these objects as metrics of criticality for network components (see [7, 29, 43]). However, these objects cannot be applied to describe the critical network components in our game due to the heterogeneity of path interdiction probabilities resulting from the transportation costs. A related issue is that computing a Nash equilibrium of our game is hard because of the large size of the players' action sets. Indeed, player 1 (resp. player 2) chooses a probability

distribution over an infinite number of feasible flows (resp. exponential number of subsets of edges). Therefore, well-known algorithms for computing (approximate) Nash equilibria are practically inapplicable for this setting (see [69, 73]). Guo et al. [44] developed a column and constraint generation algorithm to approximately solve their network security game. However, it cannot be applied to our model due to the transportation and interdiction costs that we consider.

Instead, we propose an approach for analyzing equilibria of our game based on a minimum cost circulation problem, which we denote ($\mathcal{M}$), and our existence problem on posets ($\mathcal{D}$). In particular, we show (Proposition 13) that Nash equilibria of the game can be described using primal and dual optimal solutions of ($\mathcal{M}$), if they satisfy the following conditions: (i) each network edge is interdicted with probability given by the corresponding optimal dual variable; and (ii) each source-destination path is interdicted with some probability, derived from the properties of the network, as well as the optimal dual solution. In fact, this problem is an instantiation of problem ($\mathcal{D}$), and an equilibrium interdiction strategy can be constructed with our combinatorial algorithm (Algorithm 1). We show that in some cases, this algorithm can be refined to run in polynomial time.

The main insights from our equilibrium analysis are as follows:

1. An equilibrium strategy for player 1 is given by an optimal flow of ($\mathcal{M}$), and marginal edge interdiction probabilities resulting from player 2's equilibrium strategy are given by the dual solutions of ($\mathcal{M}$). This result circumvents the complexity of equilibrium computation for our game-theoretic model. Computing an equilibrium interdiction strategy with our algorithm is NP-hard due to the enumeration of exponentially many maximal chains. However, the marginal edge interdiction probabilities and route flows can be obtained in polynomial time by solving the minimum cost circulation problem ($\mathcal{M}$) (see [59, 82]).

2. Primal-dual pairs of solutions of ($\mathcal{M}$) that satisfy strict complementary slackness provide a new characterization of the critical components in the network. Specifically, the primal (resp. dual) solution provides the paths (resp. edges)

that are chosen (resp. interdicted) in at least one Nash equilibrium of the game (Theorem 6). This result generalizes the classical min-cut-based metrics of network criticality previously studied in the network interdiction literature (see [8, 74, 112, 115]). Indeed, we show that in our more general setting, multiple edges in a source-destination path may be interdicted in equilibrium, and cannot be represented with a single cut of the network. We address this issue by computing the dual solutions of $(\mathcal{M})$ and by constructing an equilibrium interdiction strategy using our combinatorial algorithm (Algorithm 1) for posets.

The rest of the chapter is organized as follows: In Section 3.2, we pose our existence problem on posets, and introduce our main feasibility result. Section 3.3 constructs a solution to the existence problem. The implications of our existence result are then demonstrated in Section 3.4, where we study our generic network security game. Lastly, we provide some concluding remarks in Section 3.5, and the complete proofs of our results are provided in Section 3.6.

3.2 Problem Formulation and Main Result

In this section, we first recall some standard definitions in order theory. We then pose our problem of proving the existence of probability distributions over partially ordered sets, and introduce our main result about its feasibility.

3.2.1 Order Theoretic Definitions

A finite *partially ordered set* or *poset* P is a pair $(X, \preceq)$, where X is a finite set and $\preceq$ is a partial order on X, i.e., $\preceq$ is a binary relation on X satisfying:

- Reflexivity: $\forall x \in X,\ x \preceq x$ in P.
- Antisymmetry: $\forall (x, y) \in X^2$, if $x \preceq y$ in P and $y \preceq x$ in P, then $x = y$.
- Transitivity: $\forall (x, y, z) \in X^3$, if $x \preceq y$ in P and $y \preceq z$ in P, then $x \preceq z$ in P.

Given $(x, y) \in X^2$, we denote $x \prec y$ in P if $x \preceq y$ in P and $x \neq y$. We say that x and y are *comparable* in P if either $x \prec y$ in P or $y \prec x$ in P. On the other hand, x and y are *incomparable* in P if neither $x \prec y$ in P nor $y \prec x$ in P. We say that x is *covered* in P by y, denoted $x \prec\!: y$ in P, if $x \prec y$ in P and there does not exist $z \in X$ such that $x \prec z$ in P and $z \prec y$ in P. When there is no confusion regarding the poset, we abbreviate $x \preceq y$ in P by writing $x \preceq y$, etc.

Let Y be a nonempty subset of X, and let $\preceq_{|_Y}$ denote the restriction of $\preceq$ to Y. Then, $\preceq_{|_Y}$ is a partial order on Y, and $(Y, \preceq_{|_Y})$ is a *subposet* of P. A poset $P = (X, \preceq)$ is called a *chain* (resp. *antichain*) if every distinct pair of elements in X is comparable (resp. incomparable) in P. Given a poset $P = (X, \preceq)$, a nonempty subset $Y \subseteq X$ is a *chain* (resp. an *antichain*) in P if the subposet $(Y, \preceq_{|_Y})$ is a chain (resp. an antichain). A single element of X is both a chain and an antichain.

Given a poset $P = (X, \preceq)$, an element $x \in X$ is a *minimal* element (resp. *maximal* element) if there are no elements $y \in X$ such that $y \prec x$ (resp. $x \prec y$). Note that any chain has a unique minimal and maximal element. A chain $C \subseteq X$ (resp. antichain $A \subseteq X$) is *maximal* in P if there are no other chains C' (resp. antichains A') in P that contain C (resp. A). Let $\mathcal{C}$ and $\mathcal{A}$ respectively denote the set of maximal chains and antichains in P. A maximal chain $C \in \mathcal{C}$ of size n can be represented as $C = \{x_1, \ldots, x_n\}$ where $\forall k \in [\![1, n-1]\!],\ x_k \prec\!: x_{k+1}$. We state the following property:

Lemma 9. *Given a finite nonempty poset P, the set of minimal elements of P is an antichain of P, and intersects with every maximal chain of P.*

Given a poset $P = (X, \preceq)$, we consider its *cover* graph, denoted $H_P = (X, E_P)$. H_P is an undirected graph whose set of vertices is X, and whose set of edges is given by $E_P \coloneqq \{(x, y) \in X^2 \mid x \prec\!: y \text{ or } y \prec\!: x\}$. When H_P is represented such that for all $x \prec\!: y \in X$, the vertical coordinate of the vertex corresponding to y is higher than the vertical coordinate of the vertex corresponding to x, the resulting diagram is called a *Hasse diagram* of P.

We now introduce the notion of subposet generated by a subset of maximal chains. Given a poset $P = (X, \preceq)$, let $X' \subseteq X$ be a subset of elements, let $\mathcal{C}' \subseteq \mathcal{C}$ be a subset

of maximal chains of P, and consider the binary relation $\preceq_{\mathcal{C}'}$ defined by:

$$\forall (x,y) \in X'^2,\ x \preceq_{\mathcal{C}'} y \iff (x = y) \text{ or } (\exists\, C \in \mathcal{C}' \text{ such that } x, y \in C \text{ and } x \prec y).$$

Furthermore, we consider that if $C^1 = \{x_{-k}, \ldots, x_{-1}, x^*, x_1, \ldots, x_n\}$ and $C^2 = \{y_{-l}, \ldots, y_{-1}, x^*, y_1, \ldots, y_m\}$ are in $\mathcal{C}'$ and intersect in $x^* \in X'$, then $\mathcal{C}'$ also contains $C_1^2 = \{x_{-k}, \ldots, x_{-1}, x^*, y_1, \ldots, y_m\}$ and $C_2^1 = \{y_{-l}, \ldots, y_{-1}, x^*, x_1, \ldots, x_n\}$. In other words, $\mathcal{C}'$ preserves the decomposition of maximal chains intersecting in X'. Then, we have the following lemma:

Lemma 10. *Consider the poset $P = (X, \preceq)$, a subset $X' \subseteq X$, and a subset $\mathcal{C}' \subseteq \mathcal{C}$ that preserves the decomposition of maximal chains intersecting in X'. Then, $P' = (X', \preceq_{\mathcal{C}'})$ is also a poset. Furthermore, for any maximal chain C of P' of size at least two, there exists a maximal chain C' in $\mathcal{C}'$ such that $C = C' \cap X'$.*

The subposet $P' = (X', \preceq_{\mathcal{C}'})$ of P in Lemma 10 satisfies the property that if two elements in X' are comparable in P, and belong to a same maximal chain $C \in \mathcal{C}'$, then they are also comparable in P'. Graphically, this is equivalent to removing the edges from the Hasse diagram H_P if their two end nodes do not belong to a same maximal chain $C \in \mathcal{C}'$.

Example 8. Consider the poset P represented by the Hasse Diagram H_P in Figure 3-1.

Figure 3-1: On the left is represented a Hasse diagram of a poset P. On the right is represented a Hasse diagram of the subposet $P' = (X', \preceq_{\mathcal{C}'})$ of P, where $X' = \{1, 2, 3, 4, 6\}$ and $\mathcal{C}' = \{\{1, 3, 5, 6\}, \{2, 3, 5, 6\}\}$.

We observe that $1 \prec 4$, $2 \prec: 3$; 1 and 3 are comparable, but 4 and 6 are in-

comparable; $\{2,4\}$ is a chain in P, but is not maximal since it is contained in the maximal chain $\{2,3,4\}$. Similarly, $\{4\}$ is an antichain in P, but is not maximal since it is contained in the maximal antichain $\{4,5\}$. The sets of maximal chains and antichains of P are given by $\mathcal{C} = \{\{1,3,4\},\{2,3,5,6\},\{1,3,5,6\},\{2,3,4\}\}$ and $\mathcal{A} = \{\{1,2\},\{3\},\{4,5\},\{4,6\}\}$, respectively. The set of minimal elements of P is given by $\{1,2\}$, and intersects with every maximal chain in $\mathcal{C}$. Finally, $P' = (X', \preceq_{\mathcal{C}'})$, where $X' = \{1,2,3,4,6\}$ and $\mathcal{C}' = \{\{1,3,5,6\},\{2,3,5,6\}\}$, is a poset, and is illustrated in Figure 3-1. $\triangle$

3.2.2 Existence of Probability Distributions over Posets

Consider a finite nonempty poset $P = (X, \preceq)$. Let $\mathcal{P} \coloneqq 2^X$ denote the power set of X, and let $\Delta(\mathcal{P}) \coloneqq \{\sigma \in \mathbb{R}_+^{|\mathcal{P}|} \mid \sum_{S\in\mathcal{P}} \sigma_S = 1\}$ denote the set of probability distributions over $\mathcal{P}$. We are concerned with the setting where each element $x \in X$ is associated with a value $\rho_x \in [0,1]$, and each maximal chain $C \in \mathcal{C}$ has a value $\pi_C \leq 1$. Our problem is to determine if there exists a probability distribution $\sigma \in \Delta(\mathcal{P})$ such that for every element $x \in X$, the probability that x is in a subset $S \in \mathcal{P}$ is equal to ρ_x; and for every maximal chain $C \in \mathcal{C}$, the probability that C intersects with a subset $S \in \mathcal{P}$ is at least π_C. That is,

$$(\mathcal{D}): \quad \exists\, \sigma \in \mathbb{R}_+^{|\mathcal{P}|} \text{ such that } \begin{cases} \displaystyle\sum_{\{S\in\mathcal{P}\,|\,x\in S\}} \sigma_S = \rho_x, & \forall x \in X, \qquad (3.1a) \\ \displaystyle\sum_{\{S\in\mathcal{P}\,|\,S\cap C\neq\emptyset\}} \sigma_S \geq \pi_C, & \forall C \in \mathcal{C}, \qquad (3.1b) \\ \displaystyle\sum_{S\in\mathcal{P}} \sigma_S = 1. & \qquad (3.1c) \end{cases}$$

For the case in which $\pi_C \leq 0$ for all maximal chains $C \in \mathcal{C}$, constraints (3.1b) can be removed, and the feasibility of $(\mathcal{D})$ follows from Carathéodory's theorem. However, no known results can be applied to the general case. Note that although (3.1a)-(3.1c) form a polyhedral set, Farkas' lemma cannot be directly used to evaluate its feasibility. Instead, in this chapter, we study the feasibility of $(\mathcal{D})$ using order-theoretic properties of the problem. We assume two natural conditions on $\rho = (\rho_x)_{x\in X}$ and $\pi = (\pi_C)_{C\in\mathcal{C}}$,

which we introduce next.

Firstly, for feasibility of $(\mathcal{D})$, ρ and π must satisfy the following inequality:

$$\forall C \in \mathcal{C}, \quad \sum_{x \in C} \rho_x \geq \pi_C. \tag{3.2}$$

Indeed, if $(\mathcal{D})$ is feasible, then for $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ satisfying (3.1a)-(3.1c), the following holds:

$$\begin{aligned} \forall C \in \mathcal{C}, \sum_{x \in C} \rho_x &\overset{\text{(3.1a)}}{=} \sum_{x \in C} \sum_{\{S \in \mathcal{P} \,|\, x \in S\}} \sigma_S = \sum_{S \in \mathcal{P}} \sigma_S \sum_{x \in C} \mathbb{1}_{\{x \in S\}} = \sum_{S \in \mathcal{P}} \sigma_S |S \cap C| \\ &\geq \sum_{\{S \in \mathcal{P} \,|\, S \cap C \neq \emptyset\}} \sigma_S \overset{\text{(3.1b)}}{\geq} \pi_C. \end{aligned}$$

That is, the necessity of (3.2) follows from the fact that for any probability distribution over $\mathcal{P}$, and any subset of elements $C \subseteq X$, the probability that C intersects with a subset $S \in \mathcal{P}$ is upper bounded by the sum of the probabilities with which each element in C is in a subset $S \in \mathcal{P}$.

Secondly, we consider that π satisfies a specific condition for each pair of maximal chains that intersect each other. Consider any pair of maximal chains C^1 and C^2 of P, with $C^1 \cap C^2 \neq \emptyset$. Let $x^* \in C^1 \cap C^2$, and let us rewrite $C^1 = \{x_{-k}, \ldots, x_{-1}, x^*, x_1, \ldots, x_n\}$ and $C^2 = \{y_{-l}, \ldots, y_{-1}, x^*, y_1, \ldots, y_m\}$. Then, P also contains two maximal chains $C_1^2 = \{x_{-k}, \ldots, x_{-1}, x^*, y_1, \ldots, y_m\}$ and $C_2^1 = \{y_{-l}, \ldots, y_{-1}, x^*, x_1, \ldots, x_n\}$ that satisfy $C^1 \cup C^2 = C_1^2 \cup C_2^1$; see Figure 3-2 for an illustration. We require that π satisfy the following condition:

$$\pi_{C^1} + \pi_{C^2} = \pi_{C_1^2} + \pi_{C_2^1}. \tag{3.3}$$

Thus, (3.3) can be viewed as a *conservation law* on the maximal chains in $\mathcal{C}$.

We now present our main result regarding the feasibility of $(\mathcal{D})$, under conditions (3.2) and (3.3).

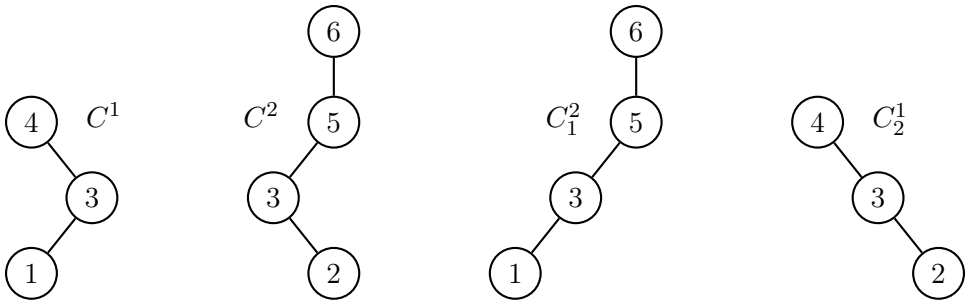


Figure 3-2: Four maximal chains of the poset shown in Figure 3-1.

Theorem 4. *The problem* $(\mathcal{D})$ *is feasible for any finite nonempty poset* $(X, \preceq)$*, with parameters* $\rho = (\rho_x) \in [0,1]^{|X|}$ *and* $\pi = (\pi_C) \in]-\infty, 1]^{|\mathcal{C}|}$ *that satisfy* (3.2) *and* (3.3)*.*

This result plays a crucial role in solving a generic formulation of network security game, which we study in Section 3.4. The game involves two players: a "router" who sends a flow of goods to maximize her value of flow crossing the network while facing transportation costs; and an "interdictor" who inspects one or more network edges to maximize the value of interdicted flow while facing interdiction costs. Our analysis in Section 3.4 shows that if a randomized network interdiction strategy interdicts each edge x with a probability ρ_x, and interdicts each path C with a probability at least π_C, then it is an interdiction strategy in a Nash equilibrium. Essentially, for this game, (ρ_x) and (π_C) are governed by network properties, such as edge transportation and interdiction costs, and naturally satisfy (3.2) and (3.3). In fact, when the network is a directed acyclic graph, a partial order can be defined on the set of edges, such that the set of maximal chains is exactly the set of source-destination paths of the network. Thus, showing the existence of interdiction strategies satisfying the above-mentioned requirements is an instantiation of the problem $(\mathcal{D})$. Theorem 4 can then be used to derive several useful insights on the equilibrium strategies of this game.

Importantly, note that $(\mathcal{D})$ may not be feasible if P is not a poset. Let us consider the following example: $X = \{1,2,3\}$, $\mathcal{C} = \{\{1,2\},\{1,3\},\{2,3\}\}$, $\rho_x = 0.5$, $\forall x \in X$, and $\pi_C = 1$, $\forall C \in \mathcal{C}$. There is no poset that has $\mathcal{C}$ as its set of maximal chains. If $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ satisfies (3.1a) and (3.1b), then necessarily, $\sigma_{\{x\}} = 0.5$, $\forall x \in X$. However, this implies that $\sum_{S \in \mathcal{P}} \sigma_S \geq 1.5 > 1$, which renders $(\mathcal{D})$ infeasible for this example.

Thus, in proving Theorem 4, we consider that the problem $(\mathcal{D})$ is defined for a poset. Next, we show that $(\mathcal{D})$ is feasible if and only if the optimal value of a linear program is no more than 1.

3.2.3 Equivalent Optimization Problem

Consider the problem $(\mathcal{D})$ for a given poset $P = (X, \preceq)$, and vectors $\rho \in [0,1]^{|X|}$ and $\pi \in]-\infty, 1]^{|\mathcal{C}|}$ satisfying (3.2) and (3.3). We can observe that when $\sum_{x\in X} \rho_x \leq 1$, a trivial solution for $(\mathcal{D})$ is given by: $\widetilde{\sigma}_{\{x\}} = \rho_x$, $\forall x \in X$, and $\widetilde{\sigma}_{\emptyset} = 1 - \sum_{x\in X} \rho_x$. The vector $\widetilde{\sigma}$ so constructed indeed represents a probability distribution over $\mathcal{P}$, and satisfies constraints (3.1a). Furthermore, for each maximal chain $C \in \mathcal{C}$, $\sum_{\{S\in\mathcal{P}\,|\,S\cap C\neq\emptyset\}} \widetilde{\sigma}_S = \sum_{x\in C} \rho_x \overset{(3.2)}{\geq} \pi_C$. Therefore, $\widetilde{\sigma}$ is a feasible solution of $(\mathcal{D})$. However, in general, $\sum_{x\in X} \rho_x$ may be larger than 1, which prevents the aforementioned construction of $\widetilde{\sigma}$ from being a probability distribution. Thus, to construct a feasible solution of $(\mathcal{D})$, we need to assign some probability to subsets of elements of size larger than 1. This is governed by the following quantity:

$$\forall C \in \mathcal{C},\ \delta_C = \sum_{x\in C} \rho_x - \pi_C. \tag{3.4}$$

To highlight the role of $\delta = (\delta_C)_{C\in\mathcal{C}}$ when assigning probabilities to subsets of elements, we consider the following optimization problem:

$$\begin{aligned}
(\mathcal{Q}): \quad \text{minimize} \quad & \sum_{S\in\mathcal{P}} \sigma_S & & \\
\text{subject to} \quad & \sum_{\{S\in\mathcal{P}\,|\,x\in S\}} \sigma_S = \rho_x, & \forall x \in X & \qquad (3.5)\\
& \sum_{\{S\in\mathcal{P}\,|\,|S\cap C|\geq 2\}} \sigma_S(|S\cap C| - 1) \leq \delta_C, & \forall C \in \mathcal{C} & \qquad (3.6)\\
& \sigma_S \geq 0, & \forall S \in \mathcal{P}. &
\end{aligned}$$

Problems $(\mathcal{Q})$ and $(\mathcal{D})$ are related in that the set of constraints (3.1a)-(3.1b) is equivalent to the set of constraints (3.5)-(3.6); see the proof of Proposition 9.

Furthermore, the objective function in $(\mathcal{Q})$ is analogous to the constraint (3.1c) in $(\mathcal{D})$. The feasibility of $(\mathcal{Q})$ is straightforward (for example, $\widetilde{\sigma}$ constructed above is a feasible solution); however, a feasible solution of $(\mathcal{Q})$ may not be a probability distribution.

Note that given a maximal chain $C \in \mathcal{C}$, constraint (3.6) bounds the total amount of probability that can be assigned to subsets that contain more than one element in C. One can see that for a subset $S \in \mathcal{P}$ such that $|S \cap C| \leq 1$, the probability σ_S assigned to S does not influence constraint (3.6). However, the more elements from C a subset S contains, the smaller the probability that can be assigned to S, due to scaling by the factor $(|S \cap C| - 1)$. Thus, δ determines the amount of probability that can be assigned to larger subsets.

Let $z^*_{(\mathcal{Q})}$ denote the optimal value of $(\mathcal{Q})$. We show the following equivalence between $(\mathcal{D})$ and $(\mathcal{Q})$:

Proposition 9. *$(\mathcal{D})$ is feasible if and only if $z^*_{(\mathcal{Q})} \leq 1$.*

Therefore, proving Theorem 4 is equivalent to showing that $z^*_{(\mathcal{Q})} \leq 1$. In fact, we show a stronger result, which will be useful for our equilibrium analysis in Section 3.4.

Theorem 5. $z^*_{(\mathcal{Q})} = \max\{\max\{\rho_x,\ x \in X\}, \max\{\pi_C,\ C \in \mathcal{C}\}\}$.

It is easy to see that $z^*_{(\mathcal{Q})} \geq \max\{\max\{\rho_x,\ x \in X\}, \max\{\pi_C,\ C \in \mathcal{C}\}\}$. Indeed, any feasible solution $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ of $(\mathcal{Q})$ satisfies $\sum_{S \in \mathcal{P}} \sigma_S \geq \sum_{\{S \in \mathcal{P} \,|\, x \in S\}} \sigma_S = \rho_x,\ \forall x \in X$, and $\sum_{S \in \mathcal{P}} \sigma_S \geq \sum_{\{S \in \mathcal{P} \,|\, S \cap C \neq \emptyset\}} \sigma_S \overset{(3.24)}{\geq} \pi_C,\ \forall C \in \mathcal{C}$. To show the reversed inequality, we need to prove that there exists a feasible solution of $(\mathcal{Q})$ with objective value equal to $\max\{\max\{\rho_x,\ x \in X\}, \max\{\pi_C,\ C \in \mathcal{C}\}\}$. This is the focus of the next section.

3.3 Constructive Proof of Theorem 5

We design a combinatorial algorithm to compute a feasible solution of $(\mathcal{Q})$ with objective value exactly equal to $\max\{\max\{\rho_x,\ x \in X\}, \max\{\pi_C,\ C \in \mathcal{C}\}\}$. Recall from Section 3.2.3 that such a feasible solution is optimal for $(\mathcal{Q})$, and can be used to construct a feasible solution of $(\mathcal{D})$; see the proof of Proposition 9.

Before formally introducing our algorithm, we discuss the main ideas behind its design. In each iteration, the algorithm selects a subset of elements and assigns a positive weight to it. Let us discuss the execution of the first iteration of the algorithm.

Firstly, we need to determine the collection of subsets that can be assigned a positive weight without violating any of the constraints in the problem $(\mathcal{Q})$. Essentially, this is dictated by the maximal chains $C \in \mathcal{C}$ for which $\delta_C = 0$. Indeed, for any $C \in \mathcal{C}$ with $\delta_C = 0$, we have the following equivalence:

$$\sum_{\{S \in \mathcal{P} \,|\, |S \cap C| \geq 2\}} \underbrace{\sigma_S}_{\geq 0} \underbrace{(|S \cap C| - 1)}_{>0} \leq 0 \iff \sigma_S = 0, \ \forall S \in \mathcal{P} \text{ such that } |S \cap C| \geq 2.$$

In other words, if a maximal chain $C \in \mathcal{C}$ is such that $\delta_C = 0$ (i.e., $\sum_{x \in C} \rho_x = \pi_C$), then a vector $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ is feasible for $(\mathcal{Q})$ only if its support does *not* contain any set $S \in \mathcal{P}$ that intersects C in more than one element. Therefore, our algorithm must select a subset of elements $S \in \mathcal{P}$ that satisfies $|S \cap C| \leq 1$, for all $C \in \mathcal{C}$ such that $\delta_C = 0$.

To precisely characterize this collection of subsets, we consider the notion of subposet generated by a subset of maximal chains, introduced in Section 3.2.1. In particular, by considering $\mathcal{C}'$ the set of maximal chains $C \in \mathcal{C}$ such that $\delta_C = 0$, and X' the subset of elements $x \in X$ such that $\rho_x > 0$, we can show (in Proposition 10 below) that the condition stated in Lemma 10 is satisfied, and $P' = (X', \preceq_{\mathcal{C}'})$ is a poset. Interestingly, we can then deduce that the subsets of elements that we can select from at that iteration are the antichains of P'. In any poset, a chain and an antichain intersect in at most one element. By definition of $\preceq_{\mathcal{C}'}$, this implies that $|S \cap C| \leq 1$ for every antichain $S \subseteq X'$ of P' and every maximal chain $C \in \mathcal{C}$ of P such that $\delta_C = 0$.

Now, we need to determine which antichain of P' to select. Let $S' \subseteq X'$ denote the subset of elements selected by the algorithm in the first iteration. Recall that an optimal solution of $(\mathcal{Q})$ satisfies constraints (3.1a)-(3.1b) with the least total amount of weight assigned to subsets of elements of X. Thus, it is desirable that the weight

assigned to S' in this iteration contribute towards satisfying all constraints (3.1b). To capture this requirement, our algorithm selects S' as the set of minimal elements of P'. The selected S' is an antichain of P', intersects with every maximal chain of P, and provides further properties that enable us to prove the optimality of the algorithm.

Secondly, we discuss how to determine the maximum amount of weight w' that can be assigned to S' in the first iteration, without violating any of the constraints (3.5) and (3.6). This is governed by the remaining chains $C \in \mathcal{C}$ for which $\delta_C > 0$ and the elements constituting S'. If w' is larger than $\frac{\delta_C}{|S' \cap C|-1}$ for $C \in \mathcal{C}$ such that $|S' \cap C| \geq 2$, then the corresponding constraint (3.6) will be violated. Similarly, w' cannot be larger than ρ_x, $\forall x \in S'$. Thus, the weight that we must assign to S' is:

$$w' = \min \left\{ \min \left\{ \rho_x,\, x \in S' \right\}, \min \left\{ \frac{\delta_C}{|S' \cap C| - 1},\, C \in \mathcal{C} \,|\, \delta_C > 0 \,\text{and}\, |S' \cap C| \geq 2 \right\} \right\}.$$

At the end of the iteration, we update the vectors ρ and δ, as well as the sets of elements X' and maximal chains $\mathcal{C}'$ to consider in subsequent iterations. In particular, we will show that some maximal chains need to be removed in order to preserve the conservation law at each iteration. The algorithm terminates when there are no more elements $x \in X$ with positive ρ_x. This completes the discussion of the main points that we need to account for in designing the algorithm. We are now in the position to formally present Algorithm 1.

Algorithm 1 : Optimal solution of $(\mathcal{Q})$

Input: Finite nonempty poset $P = (X, \preceq)$, and vectors $\rho \in \mathbb{R}_+^{|X|}$, $\delta \in \mathbb{R}_+^{|\mathcal{C}|}$.

Output: Vector $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$.

A1: $\mathcal{C}^1 \leftarrow \mathcal{C}, \qquad \rho_x^1 \leftarrow \rho_x, \ \forall x \in X, \qquad \delta_C^1 \leftarrow \delta_C, \ \forall C \in \mathcal{C}^1$

A2: $X^1 \leftarrow \{x \in X \mid \rho_x^1 > 0\}, \quad \overline{\mathcal{C}}^1 \leftarrow \{C \in \mathcal{C}^1 \mid \delta_C^1 = 0\}, \quad \widehat{\mathcal{C}}^1 \leftarrow \{C \in \mathcal{C}^1 \mid \delta_C^1 > 0\}$

A3: $k \leftarrow 1$

A4: **while** $X^k \neq \emptyset$ **do**

A5: Construct the poset $P^k = (X^k, \preceq_{\overline{\mathcal{C}}^k})$

A6: Choose S^k the set of minimal elements of P^k

A7: $\sigma_{S^k} \leftarrow w^k = \min\{\min\{\rho_x^k, \ x \in S^k\}, \min\{\frac{\delta_C^k}{|S^k \cap C|-1}, \ C \in \widehat{\mathcal{C}}^k \mid |S^k \cap C| \geq 2\}\}$

A8: $\rho_x^{k+1} \leftarrow \rho_x^k - w^k \mathbb{1}_{\{x \in S^k\}}, \ \forall x \in X$

A9: $\delta_C^{k+1} \leftarrow \delta_C^k - w^k(|S^k \cap C| - 1)\mathbb{1}_{\{|S^k \cap C| \geq 2\}}, \ \forall C \in \mathcal{C}$

A10: $\mathcal{C}^{k+1} \leftarrow \{C \in \mathcal{C}^k \mid$ the minimal element of $C \cap X^k$ in P is in $S^k\}$

A11: $X^{k+1} \leftarrow \{x \in X^k \mid \rho_x^{k+1} > 0\}$

A12: $\overline{\mathcal{C}}^{k+1} \leftarrow \{C \in \mathcal{C}^{k+1} \mid \delta_C^{k+1} = 0\}, \quad \widehat{\mathcal{C}}^{k+1} \leftarrow \{C \in \mathcal{C}^{k+1} \mid \delta_C^{k+1} > 0\}$

A13: $k \leftarrow k + 1$

A14: **end while**

Let n^* denote the number of iterations of Algorithm 1. Since we have not yet shown that it terminates, we suppose that $n^* \in \mathbb{N} \cup \{+\infty\}$. For every maximal chain $C \in \mathcal{C}$, let us define the sequence $(\pi_C^k)_{k \in [\![1, n^*+1]\!]}$ induced by Algorithm 1 as follows:

$$\pi_C^1 = \pi_C, \text{ and for every } k \in [\![1, n^*]\!], \ \pi_C^{k+1} = \pi_C^k - w^k \mathbb{1}_{\{S^k \cap C \neq \emptyset\}}. \tag{3.7}$$

Given $k \in [\![1, n^* + 1]\!]$, π_C^k (resp. ρ_x^k) represents the remaining value associated with the maximal chain $C \in \mathcal{C}$ (resp. the element $x \in X$) after the first $k-1$ iterations of the algorithm. For convenience, we let $X^0 \leftarrow X$.

We now proceed with proving Theorem 5. Our proof consists of three main parts:

Part 1: Algorithm 1 is well-defined (Proposition 10);

Part 2: it terminates and outputs a feasible solution of $(\mathcal{Q})$ (Proposition 11); and

Part 3: it assigns a total weight $\sum_{k=1}^{n^*} w^k$ equal to $\max\{\max\{\rho_x, \ x \in X\}, \max\{\pi_C, \ C \in \mathcal{C}\}\}$ at termination (Proposition 12).

3.3.1 Part 1: Well-Definedness of Algorithm 1.

To show that Algorihm 1 is well-defined, we need to ensure that at each iteration $k \in [\![1, n^*]\!]$ of the algorithm, P^k is a poset. Lemma 10 can be applied to show this, provided that we are able to prove that $\overline{\mathcal{C}}^k$ preserves the decomposition of maximal chains intersecting in X^k. This property, and some associated results, are stated below:

Proposition 10. *Each iteration of Algorithm 1 is well-defined. In particular, for every $k \in [\![1, n^* + 1]\!]$, the following hold:*

(i) For every maximal chain $C \in \mathcal{C}$, δ_C^k determines the remaining weight that can be assigned to subsets that intersect C at more than one element:

$$\forall C \in \mathcal{C}, \quad \delta_C^k = \sum_{x \in C} \rho_x^k - \pi_C^k, \tag{3.8}$$

$$\forall C \in \mathcal{C}^k, \quad \delta_C^k \geq 0. \tag{3.9}$$

(ii) $\mathcal{C}^k$ *preserves the decomposition of maximal chains intersecting in* X^{k-1}*:*

$$\forall (C^1, C^2) \in \mathcal{C}^2 \mid C^1 \cap C^2 \cap X^{k-1} \neq \emptyset,\ (C^1, C^2) \in (\mathcal{C}^k)^2 \Longrightarrow (C^2_1, C^1_2) \in (\mathcal{C}^k)^2.$$

(iii) π^k *satisfies the conservation law on the maximal chains of* $\mathcal{C}^k$ *that intersect in* X^{k-1}*:*

$$\forall (C^1, C^2) \in (\mathcal{C}^k)^2 \mid C^1 \cap C^2 \cap X^{k-1} \neq \emptyset, \quad \pi^k_{C^1} + \pi^k_{C^2} = \pi^k_{C^2_1} + \pi^k_{C^1_2}. \tag{3.10}$$

(iv) $P^k = (X^k, \preceq_{\overline{\mathcal{C}}^k})$ *is a poset.*

The proof of Proposition 10 highlights the importance of our construction of $\mathcal{C}^{k+1}$ for $k \in [\![1, n^*]\!]$ as given in (A10). This step of the algorithm ensures that $\mathcal{C}^{k+1}$ preserves the decomposition of maximal chains intersecting in X^k. It also ensures that each maximal chain in $\mathcal{C}^{k+1}$ intersects S^k. A direct consequence is that π^{k+1} satisfies the conservation law on the maximal chains of $\mathcal{C}^{k+1}$ that intersect in X^k. We then deduce that $\overline{\mathcal{C}}^{k+1}$ preserves the decomposition of maximal chains intersecting in X^{k+1}, which implies that P^{k+1} is a poset (Lemma 10). The issue however is that some maximal chains in $\mathcal{C}^k$ may be removed when constructing $\mathcal{C}^{k+1}$, and we must ensure that the corresponding constraints (3.6) will still be satisfied by the output of the algorithm. This is the focus of the next part.

3.3.2 Part 2: Feasibility of Algorithm 1's Output.

Now that we have shown the algorithm to be well-defined, the second main part of the proof of Theorem 5 is to show that the algorithm terminates, and outputs a feasible solution of $(\mathcal{Q})$. Showing that the algorithm terminates is based on the fact that there are finite numbers of elements and maximal chains. To show the feasibility of the solution generated by the algorithm, we need to verify that constraints (3.5) and (3.6) are satisfied. From (A11), we deduce that constraints (3.5) are automatically satisfied at termination, since an element $x \in X$ is removed whenever the remaining value ρ^k_x is 0. Similarly, from Proposition 10, we obtain that constraints (3.6) are satisfied

for all maximal chains in $\mathcal{C}^{n^*+1}$, i.e., the maximal chains that are not removed by the algorithm. As mentioned before, the main issue in showing the feasibility of Algorithm 1's output is with regards to the constraints (3.6) corresponding to the maximal chains that have been removed at some iteration of the algorithm. For such maximal chains $C \in \mathcal{C} \backslash \mathcal{C}^{n^*+1}$, we create a finite sequence of "dominating" maximal chains, and show that constraint (3.6) being satisfied for the last maximal chain of the sequence implies that it is also satisfied for the initial maximal chain C. To carry out this argument, we essentially need the following lemma:

Lemma 11. *Consider $C^{(1)} \in \mathcal{C}$, and suppose that $\exists\, k_1 \in [\![1, n^*]\!]$ such that $C^{(1)} \in \mathcal{C}^{k_1} \backslash \mathcal{C}^{k_1+1}$ and $C^{(1)} \cap X^{k_1} \neq \emptyset$. Then, $\exists\, C^{(2)} \in \mathcal{C}^{k_1+1}$ such that $\delta^{k_1}_{C^{(1)}} \geq \delta^{k_1}_{C^{(2)}}$ and $C^{(2)} \cap X^{k_1} \supseteq C^{(1)} \cap X^{k_1}$.*

As shown in the next proposition, one of the implications of Lemma 11 is that if a maximal chain $C^{(1)}$ is removed after the k_1-th iteration of the algorithm, then there exists another maximal chain $C^{(2)}$, which dominates $C^{(1)}$ in the sense that if the output of the algorithm satisfies constraint (3.6) for $C^{(2)}$, then it also satisfies that constraint for $C^{(1)}$. Additionally, it is guaranteed that $C^{(2)}$ is not removed before the $k_1 + 1-$th iteration of the algorithm. We can now show the second main part of the proof of Theorem 5

Proposition 11. *Algorithm 1 terminates, and outputs a feasible solution of $(\mathcal{Q})$.*

The output of Algorithm 1, by design, satisfies constraints (3.5), and also constraints (3.6) for the maximal chains in $\mathcal{C}^{n^*+1}$. Recall that the remaining maximal chains were removed after an iteration k in order to maintain the conservation law on the resulting set $\mathcal{C}^{k+1}$. This conservation law played an essential role in proving Proposition 11, i.e., in showing that constraints (3.6) are also satisfied for the maximal chains that are not in $\mathcal{C}^{n^*+1}$ (see the proof of Lemma 11). Thus, Algorithm 1's output is a feasible solution of $(\mathcal{Q})$. Next, we show that this solution is optimal.

3.3.3 Part 3: Optimality of Algorithm 1.

The final part of the proof of Theorem 5 consists in showing that the total weight used by the algorithm is exactly $\max\{\max\{\rho_x,\ x \in X\}, \max\{\pi_C,\ C \in \mathcal{C}\}\}$. This is done by considering the following quantity:

$$\forall k \in [\![1, n^* + 1]\!],\ W^k \coloneqq \max\{\max\{\rho_x^k,\ x \in X\}, \max\{\pi_C^k,\ C \in \mathcal{C}\}\}.$$

First, we show that $\forall k \in [\![1, n^*]\!]$, $W^{k+1} = W^k - w^k$. Then, we show that $W^{n^*+1} = 0$. Using a telescoping series, we obtain the desired result. This part of the proof also uses Lemma 11 to conclude that $\max\{\pi_C^k,\ C \in \mathcal{C}\}$ is attained by a maximal chain $C \in \mathcal{C}^{k+1}$.

Proposition 12. *The total weight used by the algorithm when it terminates is:*

$$\max\{\max\{\rho_x,\ x \in X\}, \max\{\pi_C,\ C \in \mathcal{C}\}\}.$$

In conclusion, Propositions 10, 11, and 12 enable us to show that Algorithm 1 outputs a feasible solution of $(\mathcal{Q})$ with objective value equal to $\max\{\max\{\rho_x,\ x \in X\}, \max\{\pi_C,\ C \in \mathcal{C}\}\}$. Therefore $z^*_{(\mathcal{Q})} \leq \max\{\max\{\rho_x,\ x \in X\}, \max\{\pi_C,\ C \in \mathcal{C}\}\}$. Since we already established the reversed inequality at the end of Section 3.2.3, we conclude that $z^*_{(\mathcal{Q})} = \max\{\max\{\rho_x,\ x \in X\}, \max\{\pi_C,\ C \in \mathcal{C}\}\}$, thus proving Theorem 5.

Furthermore, since $\forall x \in X,\ \rho_x \leq 1$, and $\forall C \in \mathcal{C},\ \pi_C \leq 1$, then $z^*_{(\mathcal{Q})} \leq 1$. From Proposition 9, this implies that $(\mathcal{D})$ is feasible: Given the output σ of Algorithm 1, $\widehat{\sigma}$ obtained from σ by additionally assigning $1 - z^*_{(\mathcal{Q})}$ to $\emptyset$ satisfies (3.1a)-(3.1c), and proves Theorem 4.

We illustrate Algorithm 1 with the following example:

Example 9. Consider the poset P represented by the Hasse diagram given in Figure 3-3.

In this poset P, the set of maximal chains is given by $\mathcal{C} = \{\{1, 3, 4\}, \{2, 3, 5\}, \{1, 3, 5\}, \{2, 3, 4\}\}$. We assume that the values assigned to each maximal chain are

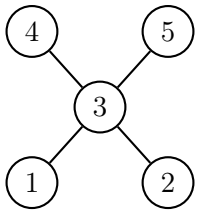


Figure 3-3: Hasse diagram of a poset P.

$\pi_{134} = \pi_{135} = 0.8$ and $\pi_{234} = \pi_{235} = 0.6$, and the values assigned to each element are $\rho_1 = 0.4$, $\rho_2 = 0.3$, $\rho_3 = 0.5$, $\rho_4 = 0.5$, $\rho_5 = 0.7$.

First, we can see that $\forall C \in \mathcal{C},\ \sum_{x \in C} \rho_x \geq \pi_C$, and $\pi_{134} + \pi_{235} = \pi_{135} + \pi_{234}$. Therefore, conditions (3.2) and (3.3) are satisfied, and we can run Algorithm 1 to optimally solve $(\mathcal{Q})$ (and construct a feasible solution of $(\mathcal{D})$). Figure 3-4a (resp. Figure 3-4b), illustrates each iteration of the algorithm using the poset P (resp. the posets P^k, for $k \in [\![1, n^*]\!]$).

- $\boldsymbol{k = 1}$ **:** $X^1 = X = [\![1, 5]\!]$, $\mathcal{C}^1 = \mathcal{C}$, $\rho_x^1 = \rho_x,\ \forall x \in X$. Note that $\delta_{134} = 0.6,\ \delta_{235} = 0.9,\ \delta_{135} = 0.8$, and $\delta_{234} = 0.7$. Since $\forall C \in \mathcal{C},\ \delta_C^1 = \delta_C > 0$, then $\overline{\mathcal{C}}^1 = \emptyset$, and $\widehat{\mathcal{C}}^1 = \mathcal{C}$. Therefore, each pair of elements in $P^1 = (X^1, \preceq_{\overline{\mathcal{C}}^1})$ is incomparable, and $S^1 = \{1, 2, 3, 4, 5\}$. Then one can check that $\min_{x \in S^1} \rho_x^1 = 0.3$ and $\min_{\{C \in \widehat{\mathcal{C}}^1 \,|\, |S^1 \cap C| \geq 2\}} \frac{\delta_C^1}{|S^1 \cap C| - 1} = 0.3$. Therefore, $\sigma_{S^1} = w^1 = 0.3 = \rho_2^1 = \frac{\delta_{134}^1}{|S^1 \cap \{1,3,4\}| - 1}$.

  Next, the values are updated as follows: $\rho_1^2 = 0.1,\ \rho_2^2 = 0,\ \rho_3^2 = 0.2,\ \rho_4^2 = 0.2,\ \rho_5^2 = 0.4$, and $\delta_{134}^2 = 0,\ \delta_{235}^2 = 0.3,\ \delta_{135}^2 = 0.2,\ \delta_{234}^2 = 0.1$. Since each maximal chain's minimal element is in S^1, then $\mathcal{C}^2 = \mathcal{C}$. We conclude the first iteration of the algorithm by letting $X^2 = \{1, 3, 4, 5\}$, $\overline{\mathcal{C}}^2 = \{\{1, 3, 4\}\}$, and $\widehat{\mathcal{C}}^2 = \{\{2, 3, 5\}, \{1, 3, 5\}, \{2, 3, 4\}\}$.

- $\boldsymbol{k = 2}$ **:** The set of minimal elements of the new poset $P^2 = (X^2, \preceq_{\overline{\mathcal{C}}^2})$ is given by $S^2 = \{1, 5\}$ (see Figure 3-4b). Furthermore, $\min_{x \in S^2} \rho_x^2 = 0.1$ and $\min_{\{C \in \widehat{\mathcal{C}}^2 \,|\, |S^2 \cap C| \geq 2\}} \frac{\delta_C^2}{|S^2 \cap C| - 1} = 0.2$, which imply that $\sigma_{S^2} = w^2 = 0.1 = \rho_1^2$. Then, the values are updated as follows: $\rho_1^3 = 0,\ \rho_2^3 = 0,\ \rho_3^3 = 0.2,\ \rho_4^3 = 0.2,\ \rho_5^3 = 0.3$, and $\delta_{134}^3 = 0,\ \delta_{235}^3 = 0.3,\ \delta_{135}^3 = 0.1,\ \delta_{234}^3 = 0.1$.

Now, one can see that the minimal element of $\{2,3,5\} \cap X^2$ and $\{2,3,4\} \cap X^2$ in P is 3, which does not belong to S^2. Therefore, $\mathcal{C}^3 = \{\{1,3,4\},\{1,3,5\}\}$. The new sets are then given by $X^3 = \{3,4,5\}$, $\overline{\mathcal{C}}^3 = \{\{1,3,4\}\}$, and $\widehat{\mathcal{C}}^3 = \{\{1,3,5\}\}$.

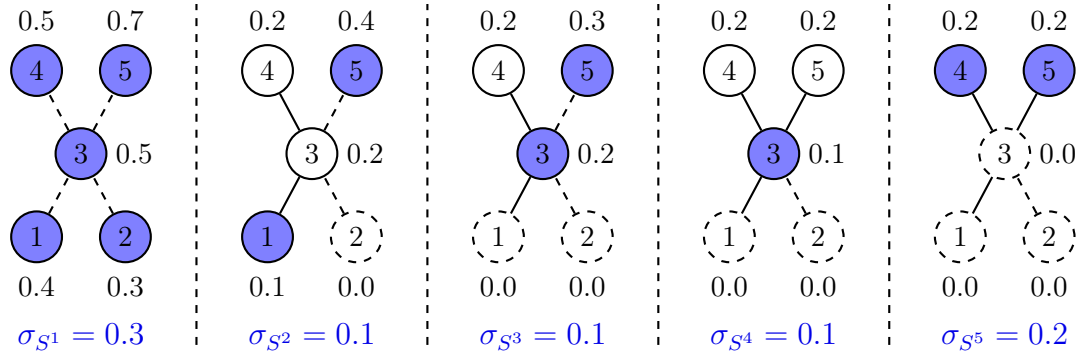
- $\boldsymbol{k = 3}$ **:** The set of minimal elements of $P^3 = (X^3, \preceq_{\overline{\mathcal{C}}^3})$ is given by $S^3 = \{3,5\}$ (see Figure 3-4b). Since $\min_{x \in S^3} \rho_x^3 = 0.2$, and $\min_{\{C \in \widehat{\mathcal{C}}^3 \,|\, |S^3 \cap C| \geq 2\}} \frac{\delta_C^3}{|S^3 \cap C|-1} = 0.1$, then $\sigma_{S^3} = w^3 = 0.1 = \frac{\delta_{135}^3}{|S^3 \cap \{1,3,5\}|-1}$. The values are updated as follows: $\rho_1^4 = 0,\ \rho_2^4 = 0,\ \rho_3^4 = 0.1,\ \rho_4^4 = 0.2,\ \rho_5^4 = 0.2$, and $\delta_{134}^4 = 0,\ \delta_{235}^4 = 0.2,\ \delta_{135}^4 = 0,\ \delta_{234}^4 = 0.1$. Then, $X^4 = \{3,4,5\}$, $\mathcal{C}^4 = \mathcal{C}^3$, $\overline{\mathcal{C}}^4 = \{\{1,3,4\},\{1,3,5\}\}$, and $\widehat{\mathcal{C}}^4 = \emptyset$.

- $\boldsymbol{k = 4}$ **:** The set of minimal elements of $P^4 = (X^4, \preceq_{\overline{\mathcal{C}}^4})$ is $S^4 = \{3\}$ (see Figure 3-4b). Then, $\sigma_{S^4} = w^4 = \min_{x \in S^4} \rho_x^4 = \rho_3^4 = 0.1$, and the new values are: $\rho_1^5 = 0,\ \rho_2^5 = 0,\ \rho_3^5 = 0,\ \rho_4^5 = 0.2,\ \rho_5^5 = 0.2$, and $\delta_C^5 = \delta_C^4,\ \forall C \in \mathcal{C}$. The new sets are $X^5 = \{4,5\}$, $\mathcal{C}^5 = \mathcal{C}^4$, $\overline{\mathcal{C}}^5 = \{\{1,3,4\},\{1,3,5\}\}$, and $\widehat{\mathcal{C}}^5 = \emptyset$.

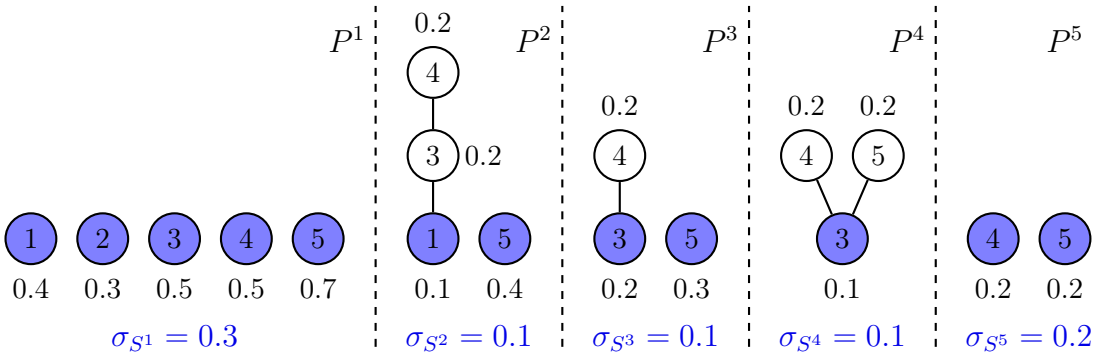
- $\boldsymbol{k = 5}$ **:** The set of minimal elements of $P^5 = (X^5, \preceq_{\overline{\mathcal{C}}^5})$ is given by $S^5 = \{4,5\}$ (Figure 3-4b), and the weight associated with it is $\sigma_{S^5} = w^5 = \rho_4^5 = \rho_5^5 = 0.2$. The updated values are given by: $\rho_x^6 = 0,\ \forall x \in X$, and $\delta_C^6 = \delta_C^5,\ \forall C \in \mathcal{C}$.

Since $X^6 = \emptyset$, the algorithm terminates, and outputs σ. One can check that σ satisfies constraints (3.5) and (3.6), and has a total weight $\sum_{S \in \mathcal{P}} \sigma_S$ of $0.8 = \max\{\max\{\rho_x,\ x \in X\}, \max\{\pi_C,\ C \in \mathcal{C}\}\}$. Therefore, from Theorem 5, σ is an optimal solution of $(\mathcal{Q})$. Since $0.8 \leq 1$, then $\widehat{\sigma} \in \mathbb{R}_+^{|\mathcal{P}|}$ given by $\widehat{\sigma}_S = \sigma_S,\ \forall S \in \mathcal{P} \backslash \emptyset$, and $\widehat{\sigma}_\emptyset = 0.2$, is a feasible solution of $(\mathcal{D})$.

$\triangle$



(a) Poset P at the beginning of each iteration of the algorithm. The solid nodes are in X^k, the dashed nodes are in $X \backslash X^k$, and the blue nodes are in S^k. An edge is solid if there exists a maximal chain in $\overline{\mathcal{C}}^k$ that contains both end nodes of the edge. The values ρ_x^k are given next to each element.



(b) P^k, for $k \in [\![1, 5]\!]$. The values ρ_x^k are given next to each element. S^k is given by the blue nodes.

Figure 3-4: Illustration of Algorithm 1 for the poset P given in Figure 3-3.

3.4 Applications to Network Security

In this section, we use Theorem 4 on the existence of probability distributions on posets for the purpose of equilibrium analysis of a generic security game. The game involves a routing entity and an interdictor interacting on a flow network.

3.4.1 Game-Theoretic Model

Consider a flow network, modeled as a directed connected acyclic graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ (resp. $\mathcal{E}$) represents the set of nodes (resp. the set of edges) of the network. For each edge $(i,j) \in \mathcal{E}$, let $c_{ij} \in \mathbb{R}_+^*$ denote its capacity. We consider that a single commodity can flow in $\mathcal{G}$ from a source node $s \in \mathcal{V}$ to a destination node $t \in \mathcal{V}$. An $s-t$ path λ of size n is a sequence of edges $\{e_1 = (s_1, t_1), \ldots, e_n = (s_n, t_n)\}$ such that $s_1 = s$, $t_n = t$, and for all $k \in [\![1, n-1]\!]$, $t_k = s_{k+1}$. We denote Λ the set containing all $s-t$ paths of $\mathcal{G}$.

A flow, defined by the vector $f \in \mathbb{R}_+^{|\Lambda|}$, enters the network from s and leaves from t. A flow f is said to be feasible if the flow through each edge does not exceed its capacity; that is, for all $(i,j) \in \mathcal{E}$, $f_{ij} \coloneqq \sum_{\{\lambda \in \Lambda \,|\, (i,j) \in \lambda\}} f_\lambda \leq c_{ij}$. Let $\mathcal{F}$ denote the set of feasible flows of $\mathcal{G}$. Given a feasible flow $f \in \mathcal{F}$, let $\mathrm{F}(f) = \sum_{\lambda \in \Lambda} f_\lambda$ denote the amount of flow sent from the node s to the node t. Each edge $(i,j) \in \mathcal{E}$ is associated with a marginal transportation cost, denoted $b_{ij} \in \mathbb{R}_+^*$. Thus, for each $s-t$ path $\lambda \in \Lambda$, $b_\lambda \coloneqq \sum_{(i,j) \in \lambda} b_{ij}$ represents the cost of transporting one unit of flow through λ. Given a feasible flow $f \in \mathcal{F}$, $\mathrm{T}(f) \coloneqq \sum_{\lambda \in \Lambda} b_\lambda f_\lambda$ denotes the total transportation cost of f.

Consider a two-player strategic game $\Gamma \coloneqq \langle \{1,2\}, (\mathcal{F}, \mathcal{I}), (u_1, u_2) \rangle$, played on the flow network $\mathcal{G}$. Player 1 (**P1**) is the routing entity that chooses to route a flow $f \in \mathcal{F}$ of goods through the network, and player 2 (**P2**) is the interdictor who simultaneously chooses a subset of edges $I \in 2^{\mathcal{E}}$ to interdict. The action set for **P1** (resp. **P2**) is $\mathcal{F}$ (resp. $\mathcal{I} \coloneqq 2^{\mathcal{E}}$). For every edge $(i,j) \in \mathcal{E}$, $d_{ij} \in \mathbb{R}_+^*$ denotes the cost of interdicting (i,j). Thus, the cost of any interdiction $I \in \mathcal{I}$ is given by $\mathrm{C}(I) \coloneqq \sum_{(i,j) \in I} d_{ij}$. In this model, **P2** (resp. **P1**) gains (resp. looses) the flow that crosses the edges that are

interdicted by **P2**; furthermore, **P1** cannot re-route its flow after **P2**'s interdiction.[1] The *effective flow*, denoted f^I, when a flow f is chosen by **P1** and an interdiction I is chosen by **P2** can be expressed as follows: $\forall \lambda \in \Lambda,\ f^I_\lambda = f_\lambda \mathbb{1}_{\{\lambda \cap I = \emptyset\}}$. We also suppose that the transportation cost incurred by **P1** is for the initial flow f and not for the effective flow f^I. This modeling choice reflects a monetary transaction between the routing entity and the network owner; for example, an advance fee incurred by the routing entity for accessing and sending a quantity of flow through the edges of the network.

The payoff of **P1** is defined as the value of effective flow assessed by **P1** net the cost of transporting the initial flow: $u_1(f, I) = p_1 \, \mathrm{F}\left(f^I\right) - \mathrm{T}(f)$, where $p_1 \in \mathbb{R}^*_+$ is the marginal value of effective flow for **P1**. Similarly, the payoff of **P2** is defined as the value of interdicted flow assessed by **P2** net the cost of interdiction: $u_2(f, I) = p_2(\mathrm{F}\,(f) - \mathrm{F}\left(f^I\right)) - \mathrm{C}\,(I)$, where $p_2 \in \mathbb{R}^*_+$ is the marginal value of interdicted flow for **P2**.

We illustrate this model through an example.

Example 10. Consider the network shown in Figure 3-5. This network contains 3 paths $\lambda^1 = \{e_1, e_4\}$, $\lambda^2 = \{e_1, e_3, e_5\}$ and $\lambda^3 = \{e_2, e_5\}$.

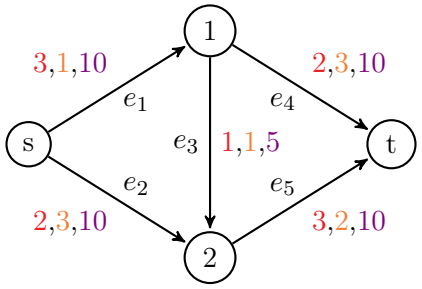
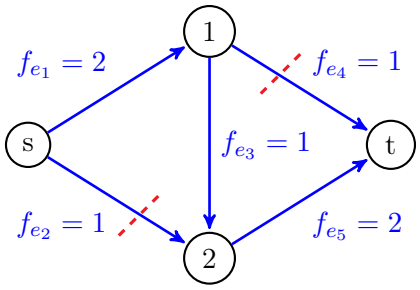


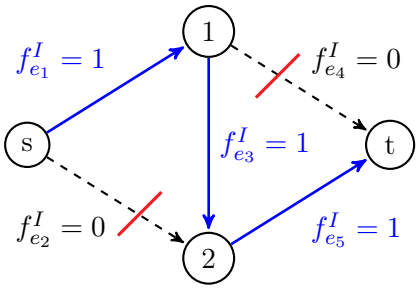
Figure 3-5: Example network. The edge labels correspond to their capacities (red), transportation costs (orange), and interdiction costs (purple).

In this example, consider that **P1** sends one unit of flow through each of the paths λ^1, λ^2 and λ^3, and **P2** interdicts edges e_2 and e_4; see Figure 3-6a. Therefore, the flows through paths λ^1 and λ^3 are interdicted and the effective flow, shown in Figure 3-6b, consists of the unit flow through the path λ^1, i.e., $\mathrm{F}\left(f^I\right) = 1$.

[1] We do not consider partial edge interdictions for the sake of simplicity.



(a) Initial flow and interdiction.



(b) Resulting effective flow.

Figure 3-6: Illustration of the game Γ.

Since 1 unit of flow crosses the network after interdiction, and the total transportation cost of f is $\mathrm{T}(f) = 13$, then **P1**'s payoff is $u_1(f, I) = p_1 - 13$. Similarly, **P2** interdicts 2 units of flow and faces an interdiction cost of $\mathrm{C}(I) = 20$. Therefore, **P2**'s payoff is $u_2(f, I) = 2p_2 - 20$. △

We consider that **P1** can route goods in the network using a flow f realized from a chosen probability distribution on the set $\mathcal{F}$, and **P2** can interdict subsets of edges according to a probability distribution on the set $\mathcal{I}$. Specifically, **P1** and **P2** respectively choose a mixed routing strategy $\sigma^1 \in \Delta(\mathcal{F})$ and a mixed interdiction strategy $\sigma^2 \in \Delta(\mathcal{I})$, where $\Delta(\mathcal{F}) = \{\sigma^1 \in \mathbb{R}_+^{|\mathcal{F}|} \mid \sum_{f\in\mathcal{F}} \sigma^1_f = 1\}$, and $\Delta(\mathcal{I}) = \{\sigma^2 \in \mathbb{R}_+^{|\mathcal{I}|} \mid \sum_{I\in\mathcal{I}} \sigma^2_I = 1\}$ denote the strategy sets. Here, σ^1_f (resp. σ^2_I) represents the probability assigned to the flow f (resp. interdiction I) by **P1**'s routing strategy σ^1 (resp. **P2**'s interdiction strategy σ^2). The players' strategies are independent randomizations. Given a strategy profile $\sigma = (\sigma^1, \sigma^2) \in \Delta(\mathcal{F}) \times \Delta(\mathcal{I})$, the respective expected payoffs are expressed as:

$$U_1(\sigma^1, \sigma^2) = p_1 \mathbb{E}_\sigma[\mathrm{F}\left(f^I\right)] - \mathbb{E}_\sigma[\mathrm{T}(f)], \tag{3.11}$$

$$U_2(\sigma^1, \sigma^2) = p_2 \left(\mathbb{E}_\sigma[\mathrm{F}\left(f\right)] - \mathbb{E}_\sigma[\mathrm{F}\left(f^I\right)]\right) - \mathbb{E}_\sigma[\mathrm{C}\left(I\right)]. \tag{3.12}$$

Thus, the mixed extension of the game Γ is $\langle\{1, 2\}, (\Delta(\mathcal{F}), \Delta(\mathcal{I})), (U_1, U_2)\rangle$.

We seek to study the mixed strategy Nash equilibria of this game. As in Section 2.2.2, a strategy profile $(\sigma^{1^*}, \sigma^{2^*}) \in \Delta(\mathcal{F}) \times \Delta(\mathcal{I})$ is a mixed strategy *Nash*

Equilibrium (NE) of game Γ if:

$$\forall \sigma^1 \in \Delta(\mathcal{F}),\ U_1(\sigma^{1^*}, \sigma^{2^*}) \geq U_1(\sigma^1, \sigma^{2^*})$$
$$\forall \sigma^2 \in \Delta(\mathcal{I}),\ U_2(\sigma^{1^*}, \sigma^{2^*}) \geq U_2(\sigma^{1^*}, \sigma^2).$$

Equivalently, in a NE $(\sigma^{1^*}, \sigma^{2^*})$, σ^{1^*} (resp. σ^{2^*}) is a best response to σ^{2^*} (resp. σ^{1^*}). We denote Σ the set of NE of Γ. We will also use the notations $U_i(\sigma^1, I) = U_i(\sigma^1, \mathbb{1}_{\{I\}})$ and $U_i(f, \sigma^2) = U_i(\mathbb{1}_{\{f\}}, \sigma^2)$ for $i \in \{1, 2\}$.

We now proceed with the equilibrium analysis of the game Γ.

3.4.2 Properties of Nash Equilibria

We first note that Γ is strategically equivalent to a zero-sum game. In particular, the following transformation preserves the set of NE. $\forall (f, I) \in \mathcal{F} \times \mathcal{I}$:

$$\frac{1}{p_1} u_1(f, I) + \frac{1}{p_2} \mathrm{C}(I) = \mathrm{F}\left(f^I\right) - \frac{1}{p_1} \mathrm{T}(f) + \frac{1}{p_2} \mathrm{C}(I) =: \widetilde{u}_1(f, I), \tag{3.13}$$
$$\frac{1}{p_2} u_2(f, I) - \mathrm{F}(f) + \frac{1}{p_1} \mathrm{T}(f) = -\widetilde{u}_1(f, I). \tag{3.14}$$

Therefore, Γ and $\widetilde{\Gamma} \coloneqq \langle \{1, 2\}, (\mathcal{F}, \mathcal{I}), (\widetilde{u}_1, -\widetilde{u}_1) \rangle$ have the same equilibrium set. Additionally, NE of Γ are interchangeable, i.e., if $(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma$ and $(\sigma^{1'}, \sigma^{2'}) \in \Sigma$, then $(\sigma^{1^*}, \sigma^{2'}) \in \Sigma$ and $(\sigma^{1'}, \sigma^{2^*}) \in \Sigma$.

In principle, NE of Γ can be obtained by using linear programming techniques. However, this would entail solving a linear program with an infinite number of variables and an exponential number of constraints (since $\mathcal{F}$ is the set of feasible flows in $\mathcal{G}$, and $|\mathcal{I}| = 2^{|\mathcal{E}|}$). We now present our approach for analyzing the NE of the game Γ. Our approach, which utilizes the existence result on posets Theorem 4, is based on a minimum cost circulation problem. Essentially, we show that its primal solutions are equilibrium routing strategies for **P1**, and that its dual solutions give properties of equilibrium interdiction strategies for **P2**.

Specifically, consider the following network flow problem:

$$
\begin{aligned}
(\mathcal{M}) \qquad \text{maximize} \quad & \mathrm{F}(f) - \frac{1}{p_1}\mathrm{T}(f) & & \\
\text{subject to} \quad & \sum_{\{\lambda\in\Lambda \,|\, (i,j)\in\lambda\}} f_\lambda \le \min\left\{\frac{d_{ij}}{p_2}, c_{ij}\right\}, & & \forall (i,j)\in\mathcal{E} \\
& f_\lambda \ge 0, & & \forall \lambda \in \Lambda.
\end{aligned}
$$

This problem can be viewed as a minimum cost circulation problem in a graph $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ such that $\mathcal{V}' = \mathcal{V}$, $\mathcal{E}' = \mathcal{E} \cup \{(t,s)\}$. The capacity of each edge $(i,j) \in \mathcal{E}$ is given by $\min\{\frac{d_{ij}}{p_2}, c_{ij}\}$, and edge (t,s) is uncapacitated. The transportation cost of each edge $(i,j) \in \mathcal{E}$ is given by $\frac{b_{ij}}{p_1}$, and the transportation cost of edge (t,s) is -1.

Equivalently, $(\mathcal{M})$ consists in finding a feasible flow f in $\mathcal{F}$ that maximizes $u_1(f, \emptyset)$ with the requirement that the flow through each edge (i,j) is no more than $\frac{d_{ij}}{p_2}$. Game theoretically, this threshold captures **P2**'s best response to **P1**: If $f_{ij} > \frac{d_{ij}}{p_2}$ for some $(i,j) \in \mathcal{E}$, then **P2** has an incentive to interdict (i,j), resulting in an increase of **P2**'s payoff (since $u_2(f, \{(i,j)\}) = p_2 f_{ij} - d_{ij} > 0$). Thus, $(\mathcal{M})$ can be viewed as the problem in which **P1** maximizes its payoff while limiting **P2**'s incentive to interdict any of the edges. For each $s-t$ path $\lambda \in \Lambda$, let us denote $\pi^0_\lambda := 1 - \frac{b_\lambda}{p_1}$. Then, the value $p_1\pi^0_\lambda$ represents the gain in **P1**'s payoff when one unit of flow traveling along λ reaches the destination node. The primal and dual formulations of $(\mathcal{M})$ are given as follows:

$$
\begin{aligned}
(\mathcal{M}_P): \quad \max \quad & \sum_{\lambda\in\Lambda} \pi^0_\lambda f_\lambda & & \\
\text{s.t.} \quad & \sum_{\{\lambda\in\Lambda \,|\, (i,j)\in\lambda\}} f_\lambda \le \frac{d_{ij}}{p_2}, & & \forall (i,j)\in\mathcal{E} \\
& \sum_{\{\lambda\in\Lambda \,|\, (i,j)\in\lambda\}} f_\lambda \le c_{ij}, & & \forall (i,j)\in\mathcal{E} \\
& f_\lambda \ge 0, & & \forall \lambda \in \Lambda
\end{aligned}
$$

$$
\begin{aligned}
(\mathcal{M}_D): \quad \min \quad & \sum_{(i,j)\in\mathcal{E}} \left(\frac{d_{ij}}{p_2}\rho_{ij} + c_{ij}\mu_{ij}\right) & \\
\text{s.t.} \quad & \sum_{(i,j)\in\lambda} (\rho_{ij} + \mu_{ij}) \geq \pi^0_\lambda, & \forall \lambda \in \Lambda \\
& \rho_{ij} \geq 0, & \forall (i,j) \in \mathcal{E} \\
& \mu_{ij} \geq 0, & \forall (i,j) \in \mathcal{E}.
\end{aligned}
$$

Let f^* and (ρ^*, μ^*) denote optimal solutions of $(\mathcal{M}_P)$ and $(\mathcal{M}_D)$, respectively. By strong duality, the optimal value of $(\mathcal{M}_P)$ is identical to that of $(\mathcal{M}_D)$; we denote it by $z^*_{(\mathcal{M})}$. Note that $(\mathcal{M}_P)$ and $(\mathcal{M}_D)$ may have an exponential number of variables and constraints, respectively. However, equivalent primal and dual formulations of $(\mathcal{M})$ of polynomial size can be derived as follows:

$$
\begin{aligned}
(\mathcal{M}'_P) \quad \text{maximize} \quad & \sum_{\{i\in\mathcal{V}\,|\,(i,t)\in\mathcal{E}\}} f_{it} - \sum_{(i,j)\in\mathcal{E}} \frac{b_{ij}}{p_1} f_{ij} & \\
\text{subject to} \quad & \sum_{\{j\in\mathcal{V}\,|\,(j,i)\in\mathcal{E}\}} f_{ji} = \sum_{\{j\in\mathcal{V}\,|\,(i,j)\in\mathcal{E}\}} f_{ij}, & \forall i \in \mathcal{V}\backslash\{s,t\} \\
& 0 \leq f_{ij} \leq c_{ij}, & \forall (i,j) \in \mathcal{E} \\
& 0 \leq f_{ij} \leq \frac{d_{ij}}{p_2}, & \forall (i,j) \in \mathcal{E}.
\end{aligned}
$$

$$
\begin{aligned}
(\mathcal{M}'_D) \quad \text{minimize} \quad & \sum_{(i,j)\in\mathcal{E}} c_{ij}\rho_{ij} + \frac{d_{ij}}{p_2}\mu_{ij} & \\
\text{subject to} \quad & y_i - y_j + \rho_{ij} + \mu_{ij} \geq -\frac{b_{ij}}{p_1}, & \forall (i,j) \in \mathcal{E} \mid i \neq s \text{ and } j \neq t \\
& -y_j + \rho_{sj} + \mu_{sj} \geq -\frac{b_{sj}}{p_1}, & \forall j \in \mathcal{V} \mid (s,j) \in \mathcal{E} \\
& y_i + \rho_{it} + \mu_{it} \geq 1 - \frac{b_{it}}{p_1}, & \forall i \in \mathcal{V} \mid (i,t) \in \mathcal{E} \\
& \rho_{ij} \geq 0, & \forall (i,j) \in \mathcal{E} \\
& \mu_{ij} \geq 0, & \forall (i,j) \in \mathcal{E}.
\end{aligned}
$$

We show the following relation between the equivalent primal and dual formulations of $(\mathcal{M})$:

Lemma 12. *Any $s-t$ path decomposition of any optimal solution f' of $(\mathcal{M}'_P)$ is an optimal solution of $(\mathcal{M}_P)$. Furthermore, given any optimal solution (ρ', μ', y') of $(\mathcal{M}'_D)$, (ρ', μ') is an optimal solution of $(\mathcal{M}_D)$.*

Thus, f^* and (ρ^*, μ^*) can be computed in an efficient manner by using an interior point method (Karmarkar [59]) or a dual network simplex algorithm (Orlin et al. [82]).

We illustrate the network flow problem $(\mathcal{M})$ with an example.

Example 11. Consider the network represented in Figure 3-5. Recall that this network contains 3 paths $\lambda^1 = \{e_1, e_4\}$, $\lambda^2 = \{e_1, e_3, e_5\}$ and $\lambda^3 = \{e_2, e_5\}$. Consider that the marginal value of effective flow for **P1** is $p_1 = 10$, and that the marginal value of interdicted flow for **P2** is $p_2 = 5$. Therefore, $\pi^0_{\lambda^1} = 0.6$, $\pi^0_{\lambda^2} = 0.6$, $\pi^0_{\lambda^3} = 0.5$. Then, the optimal primal solution f^* of $(\mathcal{M})$ routes 2 units of flow along each of the paths λ^1 and λ^2. Furthermore, an optimal dual solution (ρ^*, μ^*) of $(\mathcal{M})$ is such that $\rho^*_{e_1} = 0.5$, $\rho^*_{e_2} = 0.3$, $\rho^*_{e_3} = 0$, $\rho^*_{e_4} = 0.1$, $\rho^*_{e_5} = 0.2$, and $\mu^*_e = 0$, for every $e \in \mathcal{E}$. They are illustrated in Figure 3-7.

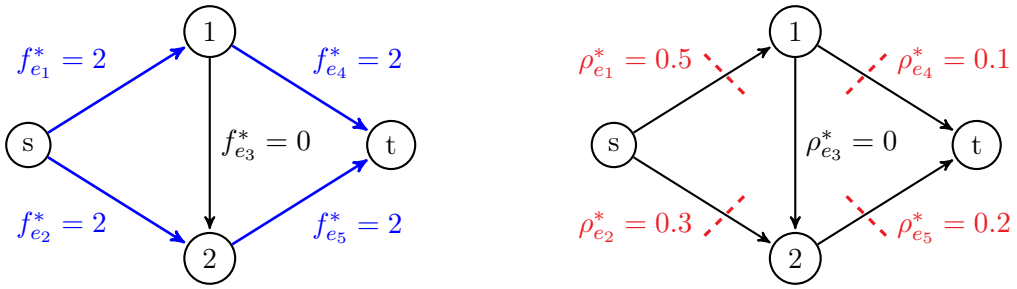


Figure 3-7: Optimal primal (left) and dual (right) solution of $(\mathcal{M})$ for the network represented in Figure 3-5, when $p_1 = 10$ and $p_2 = 5$.

Next, we define the following binary relation on $\mathcal{E}$, denoted $\preceq_{\mathcal{G}}$. Given $(u, v) \in \mathcal{E}^2$, $u \preceq_{\mathcal{G}} v$ if either $u = v$, or there exists an $s-t$ path $\lambda \in \Lambda$ that traverses u and v in this order. Since $\mathcal{G}$ is a directed acyclic connected graph, we have the following lemma:

Lemma 13. *$P = (\mathcal{E}, \preceq_{\mathcal{G}})$ is a poset, whose set of maximal chains is the set of $s-t$ paths Λ.*

Then, we recall the following properties for a pair of optimal solutions f^* and (ρ^*, μ^*) of $(\mathcal{M}_P)$ and $(\mathcal{M}_D)$ that can be obtained from complementary slackness:

$$\forall (i,j) \in \mathcal{E},\ \rho^*_{ij} > 0 \implies f^*_{ij} = \sum_{\{\lambda \in \Lambda \,|\, (i,j) \in \lambda\}} f^*_\lambda = \frac{d_{ij}}{p_2}, \tag{3.15}$$

$$\forall (i,j) \in \mathcal{E},\ \mu^*_{ij} > 0 \implies f^*_{ij} = \sum_{\{\lambda \in \Lambda \,|\, (i,j) \in \lambda\}} f^*_\lambda = c_{ij}, \tag{3.16}$$

$$\forall \lambda \in \Lambda,\ f^*_\lambda > 0 \implies \sum_{(i,j) \in \lambda} (\rho^*_{ij} + \mu^*_{ij}) = \pi^0_\lambda. \tag{3.17}$$

These properties, along with Theorem 4, enable us to derive the following result:

Proposition 13. *Consider f^* and (ρ^*, μ^*) optimal solutions of $(\mathcal{M}_P)$ and $(\mathcal{M}_D)$, respectively. Theorem 4 guarantees the existence of an interdiction strategy $\widetilde{\sigma}^2 \in \Delta(\mathcal{I})$ satisfying:*

$$\forall (i,j) \in \mathcal{E},\ \sum_{\{I \in \mathcal{I} \,|\, (i,j) \in I\}} \widetilde{\sigma}^2_I = \rho^*_{ij}, \tag{3.18}$$

$$\forall \lambda \in \Lambda,\ \sum_{\{I \in \mathcal{I} \,|\, I \cap \lambda \neq \emptyset\}} \widetilde{\sigma}^2_I \geq \pi^*_\lambda, \tag{3.19}$$

where $\forall \lambda \in \Lambda,\ \pi^*_\lambda \coloneqq \pi^0_\lambda - \sum_{(i,j) \in \lambda} \mu^*_{ij}$.

The strategy profile $(f^*, \widetilde{\sigma}^2) \in \mathcal{F} \times \Delta(\mathcal{I})$ is a NE of the game Γ. The corresponding equilibrium payoffs are $U_1(f^*, \widetilde{\sigma}^2) = p_1 \sum_{(i,j) \in \mathcal{E}} c_{ij} \mu^*_{ij}$ and $U_2(f^*, \widetilde{\sigma}^2) = 0$.

Thus, a solution f^* (resp. (ρ^*, μ^*)) of the primal (resp. dual) formulation of $(\mathcal{M})$ can be used to describe a NE of Γ. In particular, f^* is a pure equilibrium strategy for **P1**. Furthermore, for all $(i,j) \in \mathcal{E}$, ρ^*_{ij} is the probability with which edge (i,j) is interdicted by **P2** in equilibrium. To draw this conclusion, we need to show the existence of an interdiction strategy $\widetilde{\sigma}^2 \in \Delta(\mathcal{I})$ satisfying (3.18) and (3.19). In fact, this existence problem is an instantiation of problem $(\mathcal{D})$ that we introduced earlier, and positively answered in Theorem 4.

Additional properties of **P2**'s equilibrium interdiction strategy $\widetilde{\sigma}^2$ are given by μ^*: Given an $s-t$ path $\lambda \in \Lambda$, π^0_λ is the probability above which λ should be

interdicted in equilibrium by **P2**. However, when edges belonging to λ have high interdiction costs, **P2** does not interdict these edges, and may not be able to interdict λ with probability π^0_λ. The reduction of interdiction probability of λ is captured by $\sum_{(i,j)\in\lambda} \mu^*_{ij}$. Indeed, by complementary slackness (3.16), $\mu^*_{ij} > 0$ for $(i,j) \in \lambda$ only when $c_{ij} = f^*_{ij} \leq \frac{d_{ij}}{p_2}$, i.e., when the interdiction cost of (i,j) is too high. The resulting interdiction probability of λ in equilibrium is then given by $\pi^*_\lambda = \pi^0_\lambda - \sum_{(i,j)\in\lambda} \mu^*_{ij}$.

Consequently, if an $s-t$ path $\lambda \in \Lambda$ is such that $\sum_{(i,j)\in\lambda} \mu^*_{ij} > 0$, then each unit of flow sent through λ increases **P1**'s payoff by $p_1 \sum_{(i,j)\in\lambda} \mu^*_{ij}$. This is captured by **P1**'s equilibrium strategy f^*, which saturates every edge $(i,j) \in \mathcal{E}$ for which $\mu^*_{ij} > 0$ (see (3.16)). Since f^* only takes $s-t$ paths that are interdicted with probability exactly π^* (from (3.17)-(3.19)), the resulting equilibrium payoff for **P1** can then be derived from μ^*; see Proposition 13. Recall that f^* is such that interdicting any edge does not increase **P2**'s payoff. Furthermore, **P2** only interdicts edges for which the value of interdicted flow compensates the interdiction cost (from (3.15)). Thus, her payoff is 0 in equilibrium.

We note that **P1** does not need to randomize its flow in the game Γ. Indeed, for every routing strategy $\sigma^1 \in \Delta(\mathcal{F})$, the flow $\bar{f}$ defined by $\forall \lambda \in \Lambda,\ \bar{f}_\lambda = \mathbb{E}_{\sigma^1}[f_\lambda]$, satisfies the following properties: $\bar{f} \in \mathcal{F}$, and $\forall i \in \{1,2\}$, $\forall \sigma^2 \in \Delta(\mathcal{I})$, $U_i(\sigma^1, \sigma^2) = U_i(\bar{f}, \sigma^2)$.

We illustrate Proposition 13 with an example.

Example 12. Consider again the network represented in Figure 3-5, and assume that $p_1 = 10$ and $p_2 = 5$. Let f^* and (ρ^*, μ^*) be the optimal primal and dual solutions of $(\mathcal{M})$ that are represented in Figure 3-7. From Proposition 13, we deduce that the optimal primal solution f^* of $(\mathcal{M})$ is an equilibrium strategy for **P1**. Furthermore, we deduce from Theorem 4 that there exists an equilibrium interdiction strategy $\widetilde{\sigma}^2 \in \Delta(\mathcal{I})$ that interdicts every edge $(i,j) \in \mathcal{E}$ with probability ρ^*_{ij}, and every path $\lambda \in \Lambda$ with probability at least π^*_λ. In fact, this equilibrium interdiction strategy can be obtained from Algorithm 1; see Figure 3-8.

$\triangle$

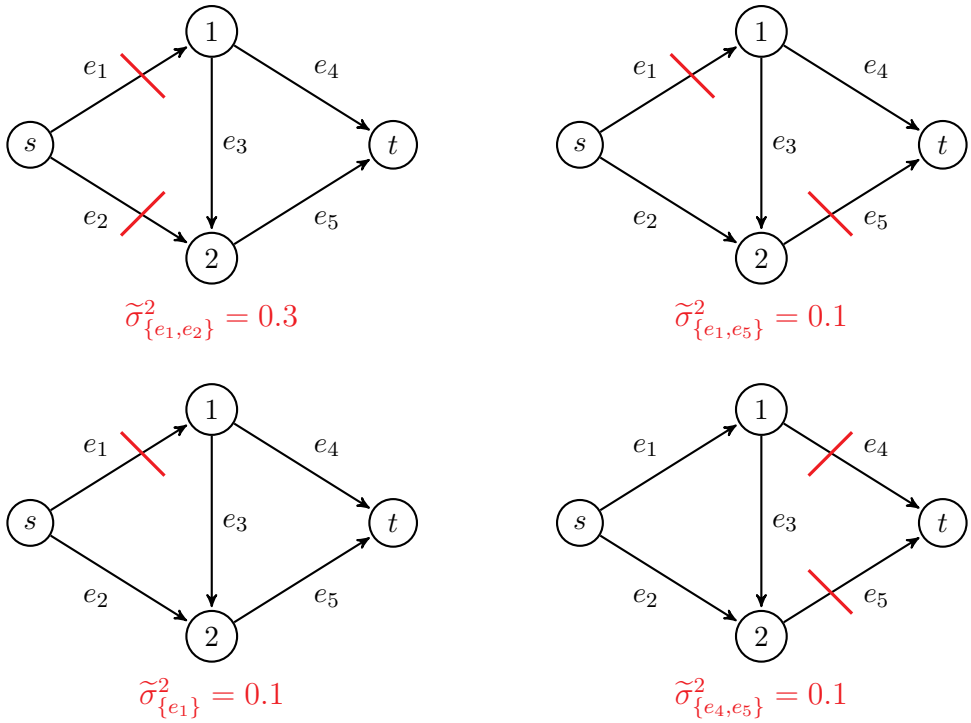


Figure 3-8: Equilibrium interdiction strategy $\widetilde{\sigma}^2$ of the game Γ on the network represented in Figure 3-5 when $p_1 = 10$ and $p_2 = 5$. Note that $\sigma^2_{\emptyset} = 0.4$.

Next, we characterize the set of $s-t$ paths (resp. set of edges) that are chosen (resp. interdicted) in at least one NE. This involves using the notion of *strict complementary slackness*. Specifically, optimal solutions $f^\dagger$ and $(\rho^\dagger, \mu^\dagger)$ of $(\mathcal{M}_P)$ and $(\mathcal{M}_D)$ satisfy strict complementary slackness if:

$$\forall (i,j) \in \mathcal{E}, \text{ either } \rho^\dagger_{ij} > 0 \text{ or } f^\dagger_{ij} = \sum_{\{\lambda \in \Lambda \,|\, (i,j) \in \lambda\}} f^\dagger_\lambda < \frac{d_{ij}}{p_2}, \tag{3.20}$$

$$\forall (i,j) \in \mathcal{E}, \text{ either } \mu^\dagger_{ij} > 0 \text{ or } f^\dagger_{ij} = \sum_{\{\lambda \in \Lambda \,|\, (i,j) \in \lambda\}} f^\dagger_\lambda < c_{ij}, \tag{3.21}$$

$$\forall \lambda \in \Lambda, \text{ either } f^\dagger_\lambda > 0 \text{ or } \sum_{(i,j) \in \lambda} (\rho^\dagger_{ij} + \mu^\dagger_{ij}) > \pi^0_\lambda. \tag{3.22}$$

We say that $f^\dagger$ and $(\rho^\dagger, \mu^\dagger)$ form a *strictly complementary primal-dual pair* of optimal solutions of $(\mathcal{M})$. Such a pair is guaranteed to exist by the Goldman-Tucker theorem [41], and can be computed using any of the existing methods in the literature (see [1, 11, 53]). From Proposition 13, we already know that there exists a NE of Γ

where **P1**'s strategy is $f^\dagger$ and **P2**'s strategy is such that each edge (i,j) is interdicted with probability $\rho^\dagger_{ij}$. In fact, we can show that $f^\dagger$ and $\rho^\dagger$ characterize the $s-t$ paths and edges that are chosen by both players in equilibrium:

Theorem 6. *Let $f^\dagger$ and $(\rho^\dagger, \mu^\dagger)$ be a strictly complementary primal-dual pair of optimal solutions of $(\mathcal{M})$. The set of $s-t$ paths (resp. the set of edges) that are chosen with positive probability by **P1**'s strategy (resp. **P2**'s strategy) in at least one NE is given by* $\text{supp}(f^\dagger)$ *(resp.* $\text{supp}(\rho^\dagger)$*):*

$$\bigcup_{(\sigma^{1^*},\sigma^{2^*})\in\Sigma} \bigcup_{f\in\text{supp}(\sigma^{1^*})} \{\lambda \in \Lambda \mid f_\lambda > 0\} = \text{supp}(f^\dagger),$$
$$\bigcup_{(\sigma^{1^*},\sigma^{2^*})\in\Sigma} \bigcup_{I\in\text{supp}(\sigma^{2^*})} I = \text{supp}(\rho^\dagger).$$

Thus, from Theorem 6, we obtain a complete characterization of the $s-t$ paths that are taken by **P1**'s equilibrium strategy, and the edges that are interdicted by **P2**'s equilibrium strategy. By computing a strictly complementary primal-dual pair $f^\dagger$ and $(\rho^\dagger, \mu^\dagger)$ of optimal solutions of $(\mathcal{M})$, the set of critical $s-t$ paths of the network is given by $\text{supp}(f^\dagger)$, and the set of critical network edges is given by $\text{supp}(\rho^\dagger)$.

We note that in the setting that we consider, **P2** may need to interdict edges that are not part of any minimum-cut set, and can even belong to different cut sets; Figure 3-9 illustrates an example. In this example, the equilibrium interdiction strategy targets edges $(s,1)$ and $(2,t)$ that do not belong to a same cut set. Thus, Theorem 6 generalizes the previously studied max-flow min-cut-based metrics of network criticality (see [7, 29, 43]).

Finally, we can derive additional equilibrium properties for the setting where each edge is potentially worth interdicting by **P2**, i.e., when $\frac{d_{ij}}{p_2} < c_{ij},\ \forall (i,j) \in \mathcal{E}$. Recall that $\frac{d_{ij}}{p_2}$ is the threshold on the flow f_{ij} that determines **P2**'s incentive to interdict edge (i,j) or not. If edge (i,j) is such that $\frac{d_{ij}}{p_2} \geq c_{ij}$, then for any feasible flow $f \in \mathcal{F}$, $f_{ij} \leq \frac{d_{ij}}{p_2}$, and interdicting that edge does not increase **P2**'s payoff. On the other hand, if $\frac{d_{ij}}{p_2} < c_{ij}$, then **P2** has an incentive to interdict (i,j) if **P1** routes more than $\frac{d_{ij}}{p_2}$ units of flow through that edge. Next, we exploit the strategic equivalence to the

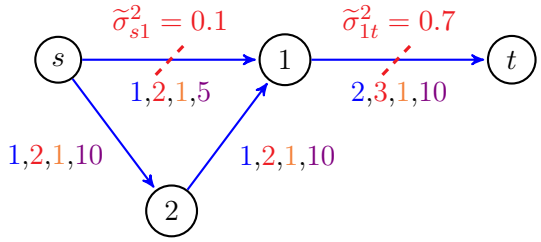


Figure 3-9: NE when $p_1 = 10$, $p_2 = 5$. The label of each edge (i, j) represents $(f^{\dagger}_{ij}, c_{ij}, b_{ij}, d_{ij})$. Edge $(s, 1)$ is interdicted by the equilibrium interdiction strategy $\widetilde{\sigma}^2$, but is not part of the minimum-cut set.

zero-sum game $\widetilde{\Gamma}$, as well as Theorems 4 and 5, to derive additional results for this special case.

Proposition 14. *If* $\forall (i,j) \in \mathcal{E}$, $\frac{d_{ij}}{p_2} < c_{ij}$, *then any NE* $\sigma^* = (\sigma^{1^*}, \sigma^{2^*}) \in \Sigma$ *satisfies the following properties:*

(i) Both players' equilibrium payoffs are constant and equal to 0.

(ii) ***P1****'s routing strategy satisfies:* $\mathbb{E}_{\sigma^{1^*}}[p_1 \mathrm{F}(f) - \mathrm{T}(f)] = p_1 z^*_{(\mathcal{M})}$.

(iii) The expected cost of ***P2****'s interdiction strategy is given by:* $\mathbb{E}_{\sigma^{2^*}}[\mathrm{C}(I)] = p_2 z^*_{(\mathcal{M})}$.

(iv) The expected amount of interdicted flow is given by: $\mathbb{E}_{\sigma^*}[\mathrm{F}(f) - \mathrm{F}(f^I)] = z^*_{(\mathcal{M})}$.

From (i)–(iv) in Proposition 14, we observe that some quantities (such as expected interdiction cost and expected amount of interdicted flow) in equilibrium can be computed in closed form using the parameters of the game and the optimal value of $(\mathcal{M})$. Thus, our results in Section 3.4 provide a new approach to study the generic security game Γ and derive equilibrium properties for settings involving heterogeneous cost parameters and general network topologies.

3.4.3 Special Cases

In Proposition 13, we showed that an interdiction strategy that satisfies (3.18) and (3.19) is an equilibrium strategy for **P2**. Although such a strategy can be constructed by utilizing Algorithm 1, it requires the enumeration of exponentially many maximal

chains of $(\mathcal{E}, \preceq_{\mathcal{G}})$ (i.e., $s-t$ paths of $\mathcal{G}$). Next, we show that in some cases, this enumeration can be avoided, thus leading to the efficient computation of an interdiction strategy in equilibrium of the game Γ.

Homogeneous Path Transportation Costs

Assume that the network $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is such that every $s-t$ path has an identical transportation cost, denoted $b \coloneqq b_\lambda$, $\forall \lambda \in \Lambda$. If $b \geq p_1$, then the game Γ is trivial: **P1**'s equilibrium strategy is not to send any flow in the network, since the transportation cost incurred for one unit of flow outweighs its value. This implies that **P2**'s equilibrium strategy is not to interdict any edge. On the other hand, if $b < p_1$, then $(\mathcal{M})$ can be viewed as a maximum flow problem in the graph $\mathcal{G}_2 = \mathcal{G}$, where the capacity of each edge $(i,j) \in \mathcal{E}$ is replaced by $\min\{\frac{d_{ij}}{p_2}, c_{ij}\}$. Let E_C be a minimum-cut set of $\mathcal{G}_2$. Furthermore, let $E_C^* = \{(i,j) \in E_C \mid \frac{d_{ij}}{p_2} < c_{ij}\}$ be the subset of edges in the minimum-cut set E_C that are potentially worth interdicting by **P2**. Then, an optimal solution of $(\mathcal{M}_D)$ is given by:

$$\forall (i,j) \in \mathcal{E},\ \rho_{ij}^* = \begin{cases} 1 - \dfrac{b}{p_1}, & \text{if } (i,j) \in E_C^*, \\ 0, & \text{otherwise,} \end{cases}$$

$$\text{and } \forall (i,j) \in \mathcal{E},\ \mu_{ij}^* = \begin{cases} 1 - \dfrac{b}{p_1}, & \text{if } (i,j) \in E_C \backslash E_C^*, \\ 0, & \text{otherwise.} \end{cases}$$

Finally, consider the interdiction strategy $\widetilde{\sigma}^2 \in \Delta(\mathcal{I})$, defined by $\widetilde{\sigma}^2_{E_C^*} = 1 - \frac{b}{p_1}$, and $\widetilde{\sigma}^2_{\emptyset} = \frac{b}{p_1}$. The strategy $\widetilde{\sigma}^2$ naturally satisfies (3.18). Additionally, consider an $s-t$ path $\lambda \in \Lambda$. By definition of a cut-set, we obtain that $\lambda \cap E_C \neq \emptyset$.

– If $\lambda \cap E_C^* \neq \emptyset$, then:

$$\sum_{\{I \in \mathcal{I} \,|\, I \cap \lambda \neq \emptyset\}} \widetilde{\sigma}^2_I = \widetilde{\sigma}^2_{E_C^*} = \pi^0_\lambda \geq \pi^*_\lambda.$$

– Otherwise, $\lambda \cap E_C \backslash E_C^* \neq \emptyset$, and $\pi^*_\lambda = \pi^0_\lambda - \sum_{(i,j)\in\lambda} \mu^*_{ij} \leq 0$.

Thus, in both cases, (3.19) is satisfied by $\widetilde{\sigma}^2$. Therefore, $\widetilde{\sigma}^2$ is an equilibrium interdiction strategy of the game Γ.

Series-Parallel Graphs

Let us consider the class of networks that can be represented as *series-parallel graphs* (SP-graphs) [30, 48]. A directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is *two-terminal series-parallel*, with terminals $s_{\mathcal{G}}$ and $t_{\mathcal{G}}$, if it can be produced by a sequence of the following operations:

1. Create a new graph, consisting of a single edge directed from $s_{\mathcal{G}}$ to $t_{\mathcal{G}}$.

2. Given two two-terminal series parallel graphs $\mathcal{H}$ and $\mathcal{K}$ with terminals $s_{\mathcal{H}}$, $t_{\mathcal{H}}$, $s_{\mathcal{K}}$, $t_{\mathcal{K}}$, form a new graph $\mathcal{G} = P_c(\mathcal{H}, \mathcal{K})$ by identifying $s_{\mathcal{G}} = s_{\mathcal{H}} = s_{\mathcal{K}}$ and $t_{\mathcal{G}} = t_{\mathcal{H}} = t_{\mathcal{K}}$. This is known as the *parallel composition* of $\mathcal{H}$ and $\mathcal{K}$.

3. Given two two-terminal series parallel graphs $\mathcal{H}$ and $\mathcal{K}$ with terminals $s_{\mathcal{H}}$, $t_{\mathcal{H}}$, $s_{\mathcal{K}}$, $t_{\mathcal{K}}$, form a new graph $\mathcal{G} = S_c(\mathcal{H}, \mathcal{K})$ by identifying $s_{\mathcal{G}} = s_{\mathcal{H}}$, $t_{\mathcal{H}} = s_{\mathcal{K}}$, and $t_{\mathcal{G}} = t_{\mathcal{K}}$. This is known as the *series composition* of $\mathcal{H}$ and $\mathcal{K}$.

We note that SP-graphs are acyclic.

An SP-graph $\mathcal{G}$ can be represented by a binary decomposition tree, which we denote $\mathcal{T}_{\mathcal{G}}$. The leafs of $\mathcal{T}_{\mathcal{G}}$ are labeled by the edges in $\mathcal{G}$. Each internal node r of $\mathcal{T}_{\mathcal{G}}$ is labeled S_c or P_c, depending on which composition is used to construct a new graph from the graphs represented by the children of r. This decomposition tree can be obtained in $O(\log(|\mathcal{V}|)^2 + \log(|\mathcal{E}|))$ time (see [48]). An example of SP-graph and its decomposition tree is represented in Figure 3-10.

First, we derive properties satisfied by primal-dual pairs of solutions of $(\mathcal{M})$ in SP-graphs.

Lemma 14. *Let (ρ^*, μ^*) be an optimal solution of $(\mathcal{M}_D)$, and let $e_1 \neq e_2 \in \mathcal{E}$ denote two edges such that $\rho^*_{e_1} > 0$ and $\rho^*_{e_2} > 0$. Let r be the root of the minimal subtree of $\mathcal{T}_{\mathcal{G}}$ that contains e_1 and e_2.*

– *If $r = P_c$, then there is no path $\lambda \in \Lambda$ such that $e_1 \in \lambda$ and $e_2 \in \lambda$.*

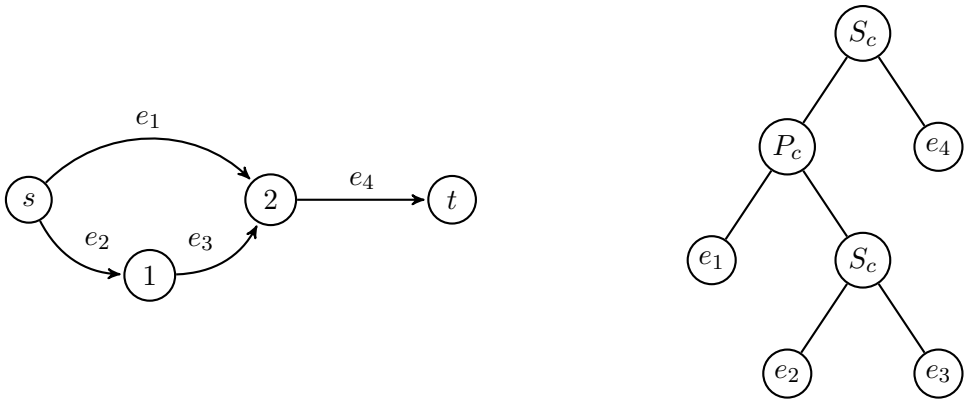


Figure 3-10: Series-parallel graph $\mathcal{G}$ (left), and its decomposition tree $\mathcal{T}_{\mathcal{G}}$ (right).

– *If $r = S_c$, then there exist an optimal solution f^* of $(\mathcal{M}_P)$ and a path $\lambda \in \Lambda$ such that $f^*_\lambda > 0$, $e_1 \in \lambda$, and $e_2 \in \lambda$.*

From this lemma, we can deduce that if two edges e_1 and e_2 are in parallel, then we can assign weight to $\{e_1, e_2\}$ without violating the set of constraints (3.6). Furthermore, if several edges $e_1, \ldots, e_n$ in the support of ρ^* are in series, then we can assign separate weights to each of them, without violating constraint (3.1c). This is possible since there exists a path $\lambda \in \Lambda \mid f^*_\lambda > 0$, which implies by complementary slackness (3.17) that:

$$\sum_{k=1}^{n} \rho^*_{e_k} \leq \sum_{(i,j)\in\lambda} \rho^*_{ij} = \pi^*_\lambda < 1.$$

Thus, given an optimal solution (ρ^*, μ^*) of $(\mathcal{M}_D)$, we can then derive an algorithm that exploits the decomposition tree $\mathcal{T}_{\mathcal{G}}$ to efficiently construct an interdiction strategy that satisfies the conditions listed above. The algorithm first assigns each leaf (i, j) of $\mathcal{T}_{\mathcal{G}}$ a vector σ^2 defined by $\sigma^2_I = \rho^*_{ij} \mathbb{1}_{\{I=(i,j)\}}$ for every $I \in \mathcal{I}$. Then, iteratively, the algorithm selects two leaves of the tree that share a same parent r. Let $\mathcal{G}_1$ and $\mathcal{G}_2$ denote the graphs represented by the leaves, and let σ^2 and $\sigma^{2'}$ be the respective associated vectors.

– If $r = S_c$ (i.e., $\mathcal{G}_1$ and $\mathcal{G}_2$ are in series in $\mathcal{G}$), then we associate the vector $\sigma^{2''} \coloneqq \sigma^2 + \sigma^{2'}$ to r.

– On the other hand, if $r = P_c$ (i.e., $\mathcal{G}_1$ and $\mathcal{G}_2$ are in parallel in $\mathcal{G}$), then we associate to r the vector $\sigma^{2''}$ defined as follows: We iteratively select $I \in \text{supp}(\sigma^2)$ and $I' \in \text{supp}(\sigma^{2'})$, and associate the weight $\min\{\sigma^2_I, \sigma^{2'}_{I'}\}$ to $\sigma^{2''}_{I\cup I'}$. We update the weights from σ^2 and $\sigma^{2'}$, and repeat the process until all the weights are transferred from σ^2 and $\sigma^{2'}$ to $\sigma^{2''}$.

We repeat this overall process until the tree only has one vertex.

The algorithm is formally defined in Algorithm 2.

It is easy to see that after each iteration of the algorithm, for each subgraph $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ of $\mathcal{G}$ represented by a leaf of the resulting tree, its corresponding vector σ^2 is such that:

$$\sum_{I\in\mathcal{I}} \sigma^2_I = \max_{\lambda\in\Lambda} \sum_{(i,j)\in\lambda\cap\mathcal{E}'} \rho^*_{ij}.$$

Therefore, at termination, the algorithm outputs a vector σ^2 that satisfies:

$$\sum_{I\in\mathcal{I}} \sigma^2_I = \max_{\lambda\in\Lambda} \sum_{(i,j)\in\lambda} \rho^*_{ij} \overset{(3.17)}{=} \max_{\lambda\in\Lambda} \pi^*_\lambda.$$

Thus, σ^2 is an optimal solution of $(\mathcal{Q})$. Finally, by assigning the weight $1 - \max_{\lambda\in\Lambda} \pi^*_\lambda$ to $\sigma^2_\emptyset$, we obtain that σ^2 is an equilibrium interdiction strategy of the game Γ.

We illustrate Algorithm 2 with an example:

Example 13. Consider the SP-graph represented in Figure 3-10, and suppose that an optimal solution of $(\mathcal{M}_D)$ is such that $\rho^*_{e_1} = 0.4$, $\rho^*_{e_2} = 0.2$, $\rho^*_{e_3} = 0.3$, $\rho^*_{e_4} = 0.2$. By complementary slackness, $\pi^*_{\{e_1,e_4\}} = 0.6$, and $\pi^*_{\{e_2,e_3,e_4\}} = 0.7$.

Then, the first iteration of Algorithm 2 selects nodes $\{e_2\}$ and $\{e_3\}$ of the decomposition tree $\mathcal{T}_\mathcal{G}$. Since $\{e_2\}$ and $\{e_3\}$ are in series, then the algorithm associates the vector σ^2 defined by $\sigma^2_{\{e_2\}} = 0.2$ and $\sigma^2_{\{e_3\}} = 0.3$. Next the algorithm selects nodes $\{e_1\}$ and $\{e_2, e_3\}$. Since they are in parallel, the algorithm associates the vector σ^2 defined by $\sigma^2_{\{e_1,e_2\}} = 0.2$, $\sigma^2_{\{e_1,e_3\}} = 0.2$, $\sigma^2_{\{e_3\}} = 0.1$. Finally, since $\{e_1, e_2, e_3\}$ and $\{e_4\}$

Algorithm 2 : Equilibrium Interdiction Strategy in Series-Parallel Graphs

Input: Decomposition tree $\mathcal{T}_{\mathcal{G}}$, and vector $\rho^* \in \mathbb{R}_+^{|\mathcal{E}|}$.

Output: Vector $\sigma^2 \in \mathbb{R}_+^{|\mathcal{I}|}$.

$\mathcal{T}^1 \leftarrow$ subtree of $\mathcal{T}_{\mathcal{G}}$ generated by $\text{supp}(\rho^*)$

Associate each leaf (i,j) with the vector σ^2 satisfying $\sigma_I^2 = \rho_{ij}^* \mathbb{1}_{\{I=(i,j)\}},\ \forall I \in \mathcal{I}$

$k \leftarrow 1$

while $\mathcal{T}^k$ is not the single vertex tree **do**

Take two leafs sharing the same parent. Let σ^2 and $\sigma^{2'}$ be the associated vectors.

if the parent is S_c **then**

$\sigma^{2''} \leftarrow \sigma^2 + \sigma^{2'}$

Associate $\sigma^{2''}$ with the parent S_c. Remove the children from $\mathcal{T}^k$.

else if the parent is P_c **then**

Without loss of generality, let us assume that $\sum_{I\in\mathcal{I}} \sigma_I^2 \geq \sum_{I\in\mathcal{I}} \sigma_I^{2'}$

while $\text{supp}(\sigma^{2'}) \neq \emptyset$ **do**

Select $I \in \text{supp}(\sigma^2)$ and $I' \in \text{supp}(\sigma^{2'})$

$\sigma_{I\cup I'}^{2''} \leftarrow \min\{\sigma_I^2, \sigma_{I'}^{2'}\}$

$\sigma_I^2 \leftarrow \sigma_I^2 - \min\{\sigma_I^2, \sigma_{I'}^{2'}\},\ \sigma_{I'}^{2'} \leftarrow \sigma_{I'}^{2'} - \min\{\sigma_I^2, \sigma_{I'}^{2'}\}$

end while

$\sigma_I^{2''} \leftarrow \sigma_I^2,\ \forall I \in \text{supp}(\sigma^2)$

Associate $\sigma^{2''}$ with the parent P_c. Remove the children from $\mathcal{T}^k$.

end if

$\mathcal{T}^{k+1} \leftarrow$ resulting subtree

$k \leftarrow k+1$

end while

are in series, then the algorithm associates the vector σ^2 defined by $\sigma^2_{\{e_1,e_2\}} = 0.2$, $\sigma^2_{\{e_1,e_3\}} = 0.2$, $\sigma^2_{\{e_3\}} = 0.1$, $\sigma^2_{\{e_4\}} = 0.2$. Finally, if $\sigma^2_{\emptyset} = 0.3$, then $\sigma^2 \in \Delta(\mathcal{I})$ is an equilibrium interdiction strategy for **P2**. $\triangle$

Comparability Graphs

We now consider any network, modeled as a directed connected acyclic graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, and we assume that the edge capacities, transportation costs, and interdiction costs, are such that there exists an optimal solution f^* of $(\mathcal{M}_P)$ that satisfies $f^*_{ij} > 0$, for every edge $(i,j) \in \mathcal{E}$.

This implies that there exists a path decomposition of f^* such that for every $s-t$ path $\lambda \in \Lambda$, $f^*_\lambda > 0$. From complementary slackness (3.17), we deduce that any dual solution (ρ^*, μ^*) of $(\mathcal{M})$ satisfies:

$$\forall \lambda \in \Lambda, \ \sum_{(i,j)\in\lambda} \rho^*_{ij} = \pi^0_\lambda - \sum_{(i,j)\in\lambda} \mu^*_{ij} = \pi^*_\lambda.$$

For this special case, problem $(\mathcal{Q})$, whose optimal solution provides an interdiction strategy in equilibrium of the game Γ, can be rewritten as follows:

$$\begin{aligned}
(\mathcal{R}) \quad \text{minimize} \quad & \sum_{I\in\mathcal{I}} \sigma^1_I & \\
\text{subject to} \quad & \sum_{\{I\in\mathcal{I} \,|\, (i,j)\in I\}} \sigma^1_I = \rho^*_{ij}, & \forall (i,j) \in \mathcal{E} \\
& \sigma^1_I = 0, & \forall (I,\lambda) \in \mathcal{I}\times\Lambda \mid |I\cap\lambda| \geq 2 \\
& \sigma^1_I \geq 0, & \forall I \in \mathcal{I}.
\end{aligned}$$

Recall from Lemma 13 that $P = (\mathcal{E}, \preceq_\mathcal{G})$ is a partially ordered set. We now associate to P its *comparability graph* $\mathcal{H}$, which is an undirected graph whose set of nodes is $\mathcal{E}$ and whose set of edges is given by $\{(e,e') \in \mathcal{E}^2 \mid e \preceq_\mathcal{G} e' \text{ or } e' \preceq_\mathcal{G} e\}$.

We recall that a set of nodes $I \subseteq \mathcal{E}$ in $\mathcal{H}$ is a *stable set* if any two nodes in I are not adjacent in $\mathcal{H}$. Let $\mathcal{S} \coloneqq \{I \in \mathcal{I} \mid \forall \lambda \in \Lambda, \ |I\cap\lambda| \leq 1\}$ denote the set of interdictions that can potentially be part of the support of an optimal solution of

$(\mathcal{R})$. By definition of the partial order $\preceq_{\mathcal{G}}$ (see Section 3.4.2), we then deduce that $\mathcal{S}$ is the set of stable sets of $\mathcal{H}$. Indeed, a set of nodes I in $\mathcal{H}$ is a stable set if and only if any two nodes e and e' in I are not comparable in the poset P, i.e., there is no $s-t$ path that intersects with both e and e'. This is equivalent to $|I \cap \lambda| \leq 1$, $\forall \lambda \in \Lambda$.

Surprisingly, this implies that $(\mathcal{R})$ can be viewed as a minimum-weighted fractional coloring problem on the comparability graph $\mathcal{H}$, whose primal and dual formulations are given as follows:

$$
\begin{aligned}
(\mathcal{R}_P) \quad & \text{minimize} && \sum_{I \in \mathcal{S}} \sigma_I^1 && \\
& \text{subject to} && \sum_{\{I \in \mathcal{S} \,|\, (i,j) \in I\}} \sigma_I^1 \geq \rho_{ij}^*, && \forall (i,j) \in \mathcal{E} \\
& && \sigma_I^1 \geq 0, && \forall I \in \mathcal{S}, \\
(\mathcal{R}_D) \quad & \text{maximize} && \sum_{(i,j) \in \mathcal{E}} \rho_{ij}^* y_{ij} && \\
& \text{subject to} && \sum_{(i,j) \in I} y_{ij} \leq 1, && \forall I \in \mathcal{S} \\
& && y_{ij} \geq 0, && \forall (i,j) \in \mathcal{E}.
\end{aligned}
$$

Now, we recall some graph theoretic definitions. An undirected graph is a *perfect graph* if the chromatic number of every induced subgraph equals the size of the largest clique of that subgraph. Furthermore, an undirected graph $\mathcal{G}$ is *strongly perfect* if for each induced subgraph $\mathcal{G}'$ of $\mathcal{G}$, $\mathcal{G}'$ contains a stable set that meets all maximal cliques of $\mathcal{G}$. Such a stable set is called a *strong stable set*.

Then, we know that every comparability graph is a strongly perfect graph, and every strongly perfect graph is a perfect graph [14]. In addition, problem $(\mathcal{R}_P)$ is totally dual integral if and only if $\mathcal{H}$ is a perfect graph (see [36]).

Therefore, we conclude that the optimal value of $(\mathcal{R})$ is the weight of the maximum-weighted clique in $\mathcal{H}$. Since a maximal clique in $\mathcal{H}$ corresponds to an $s-t$ path in

the directed graph $\mathcal{G}$, we obtain that the optimal value of $(\mathcal{R})$ is:

$$\max_{\lambda\in\Lambda} \sum_{(i,j)\in\lambda} \rho^*_{ij} \overset{(3.17)}{=} \max_{\lambda\in\Lambda} \pi^*_\lambda.$$

Then, an optimal solution of $(\mathcal{R}_P)$ can be obtained by using Hoàng's $O(|X|^2)$-time algorithm [50]. This algorithm iteratively selects a strong stable set of the comparability graph, and assigns weight to it while making sure that each $(i,j) \in \mathcal{E}$ does not receive a weight larger than ρ^*_{ij}. We describe the algorithm in more details in Algorithm 3.

Algorithm 3 : Equilibrium Interdiction Strategy from Comparability Graphs

Input: Comparability graph $\mathcal{H}$ of the poset $P = (\mathcal{E}, \preceq_{\mathcal{G}})$, and vector $\rho^* \in \mathbb{R}_+^{|\mathcal{E}|}$.

Output: Vector $\sigma^2 \in \mathbb{R}_+^{|\mathcal{I}|}$.

$\rho^1_{ij} \leftarrow \rho^*_{ij},\ \forall (i,j) \in \mathcal{E}, \qquad X^1 \leftarrow \text{supp}(\rho^1)$

$\mathcal{H}^1 \leftarrow$ subgraph of $\mathcal{H}$ generated by X^1

$k \leftarrow 1$

while $\mathcal{H}^k$ is not the empty graph **do**

  Select a strong stable set I^k of $\mathcal{H}^k$

  $w^k \leftarrow \min\{\rho^k_{ij},\ (i,j) \in I^k\}$

  $\sigma^2_{I^k} \leftarrow w^k, \qquad \rho^{k+1}_{ij} \leftarrow \rho^k_{ij} - w^k,\ \forall (i,j) \in I^k, \qquad \rho^{k+1}_{ij} \leftarrow \rho^k_{ij},\ \forall (i,j) \in X^k \backslash I^k$

  $X^{k+1} \leftarrow \text{supp}(\rho^{k+1})$

  $\mathcal{H}^{k+1} \leftarrow$ subgraph of $\mathcal{H}^k$ generated by X^{k+1}

  $k \leftarrow k+1$

end while

We note that since $\mathcal{H}$ is a strongly perfect graph, then each iteration of the algorithm decreases the length of each maximal clique in the graph by the weight assigned to the selected strong stable set. This explains why when the algorithm terminates, the total weight assigned to σ^2 is equal to the length of the maximal clique in $\mathcal{H}$.

We illustrate Algorithm 3 with an example.

Example 14. Consider the network in Figure 3-11.

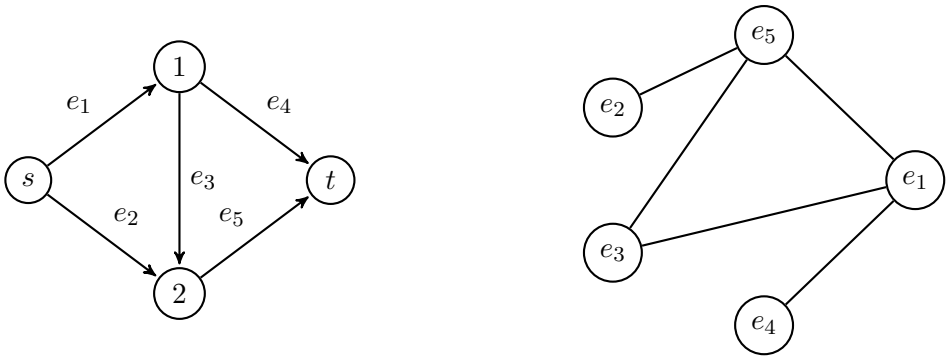


Figure 3-11: Directed acyclic graph $\mathcal{G}$ (left), and the comparability graph $\mathcal{H}$ of its corresponding poset (right).

We suppose that the parameters of the problem are such that an optimal dual solution (ρ^*, μ^*) of $(\mathcal{M})$ is such that $\rho^*_{e_1} = 0.1$, $\rho^*_{e_2} = 0.2$, $\rho^*_{e_3} = 0.2$, $\rho^*_{e_4} = 0.6$, $\rho^*_{e_5} = 0.4$. In addition, we assume that for every path λ in the network, $\sum_{(i,j)\in\lambda} \rho^*_{ij} = \pi^*_\lambda$.

The first iteration of Algorithm 3 selects the strong stable set $I^1 = \{e_2, e_3, e_4\}$, and assigns a weight $\sigma^2_{I^1} = 0.2$ to it. Then, it selects the strong stable set $I^2 = \{e_1\}$, and assigns a weight $\sigma^2_{I^2} = 0.1$. Finally, it selects the strong stable set $I^3 = \{e_4, e_5\}$, and assigns a weight $\sigma^2_{I^3} = 0.4$. Note that the algorithm used a total weight of $0.7 = \max_{\lambda\in\Lambda} \sum_{(i,j)\in\lambda} \rho^*_{ij}$. Furthermore, if we assign the weight $\sigma^2_\emptyset = 0.3$, the resulting probability distribution is an interdiction strategy in equilibrium of the game Γ.

$\triangle$

3.5 Summary

In this chapter, we studied an existence problem of probability distributions over partially ordered sets, and showed its implications to a class of security games on flow networks. In the existence problem, we considered a poset, where each element and each maximal chain is associated with a value. Under two practically relevant conditions on these values, we showed that there exists a probability distribution over the subsets of this poset, with the following properties: the probability that each element (resp. maximal chain) is contained in a subset (resp. intersects with a subset) is equal to (resp. as large as) the corresponding value. We provided a constructive

proof of this result by designing a combinatorial algorithm that exploits structural properties of the problem. We showed that in some special cases, this algorithm can be refined to run in polynomial time.

By applying this existence result, we were able to study a generic formulation of network security game between a routing entity and an interdictor. To overcome the computational and analytical challenges of the formulation, we proposed a new approach for analyzing equilibria of the game. This approach relies on our existence result on posets, as well as optimal primal and dual solutions of a minimum cost circulation problem. Furthermore, we showed that a pair of optimal solutions of the circulation problem that satisfy strict complementary slackness provides a new characterization of the critical network components that are chosen in equilibrium by both players.

3.6 Proofs of Statements

3.6.1 Proofs of Section 3.2

Proof of Lemma 9. Let P be a finite nonempty poset, and let S be the set of minimal elements of P. If $|S| = 1$, then S is an antichain of P. Now, assume that $|S| \geq 2$, and consider $x \neq y \in S$. Since x (resp. y) is a minimal element of P, then $y \not\prec x$ (resp. $x \not\prec y$). Therefore, x and y are incomparable, and S is an antichain of P.

Now, consider a maximal chain $C \in \mathcal{C}$, and assume that C does not contain any minimal element of P. Let x be the minimal element of $(C, \preceq_{|C})$. Since x is not a minimal element of P, there exists $y \in X \backslash C$ such that $y \prec x$. By transitivity of $\preceq$, we deduce that $y \prec x'$, $\forall x' \in C$. Therefore, $C \cup \{y\}$ is a chain containing C, which contradicts the maximality of C. Thus, every maximal chain of P intersects with the set of minimal elements of P. □

Proof of Lemma 10. Consider $X' \subseteq X$, and $\mathcal{C}' \subseteq \mathcal{C}$ that preserves the decomposition of maximal chains intersecting in X'. Let us show that $\preceq_{\mathcal{C}'}$ defined in Section 3.2.1 is a partial order on X':

– Reflexivity: For every $x \in X'$, $x \preceq_{\mathcal{C}'} x$ by definition.

– Antisymmetry: Consider $(x, y) \in (X')^2$ such that $x \preceq_{\mathcal{C}'} y$ and $y \preceq_{\mathcal{C}'} x$. If $x \neq y$, then we would have $x \prec y$ and $y \prec x$, which contradicts $\preceq$ being a partial order. Therefore, $x = y$.

– Transitivity: Consider $(x, y, z) \in (X')^3$, and assume that $x \preceq_{\mathcal{C}'} y$ and $y \preceq_{\mathcal{C}'} z$. If $x = y$ or $y = z$, then we trivially obtain that $x \preceq_{\mathcal{C}'} z$. Now, let us assume that $x \neq y$ and $y \neq z$. By definition of $\preceq_{\mathcal{C}'}$, $\exists\, C^1 \in \mathcal{C}' \mid (x, y) \in (C^1)^2$ and $x \prec y$. Similarly, $\exists\, C^2 \in \mathcal{C}' \mid (y, z) \in (C^2)^2$ and $y \prec z$. We can rewrite C^1 and C^2 as follows:

$$C^1 = \{x_0, \ldots, x_l = x, x_{l+1}, \ldots, x_{l+m} = y, x_{l+m+1}, \ldots, x_{l+m+n}\},$$
$$C^2 = \{y_0, \ldots, y_q = y, y_{q+1}, \ldots, y_{q+r} = z, y_{q+r+1}, \ldots, y_{q+r+s}\}.$$

Now, consider the maximal chain $C_1^2 = \{x_0, \ldots, x_l = x, x_{l+1}, \ldots, x_{l+m} = y, y_{q+1}, \ldots, y_{q+r} = z, y_{q+r+1}, \ldots, y_{q+r+s}\}$, as illustrated in Figure 3-12.

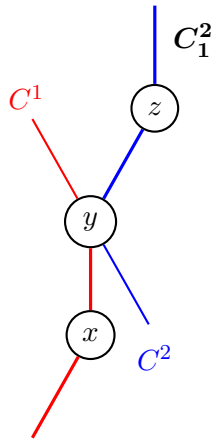


Figure 3-12: Illustration of the transitivity of $\preceq_{\mathcal{C}'}$. C_1^2 is represented by the thick chain.

Since C^1 and C^2 intersect in $y \in X'$, and $\mathcal{C}'$ preserves the decomposition of maximal chains intersecting in X', we deduce that $C_1^2 \in \mathcal{C}'$ as well. Furthermore, $(x, z) \in (C_1^2)^2$, and the transitivity of $\preceq$ implies that $x \prec z$. Therefore, $x \preceq_{\mathcal{C}'} z$.

Thus, $\preceq_{\mathcal{C}'}$ is a partial order on X', and $P' = (X', \preceq_{\mathcal{C}'})$ is a poset.

Let $C \subseteq X'$ be a maximal chain of P' of size at least two. Let us rewrite $C = \{x_1, \ldots, x_n\}$ with $n \geq 2$, where $\forall k \in [\![1, n-1]\!],\ x_k \prec\!\!:_{\mathcal{C}'} x_{k+1}$. We show by induction on $k \in [\![2, n]\!]$ that $\exists\, C' \in \mathcal{C}'$ such that $\{x_1, \ldots, x_k\} \subseteq C'$. If $k = 2$, then by definition, $\exists\, C' \in \mathcal{C}'$ such that $\{x_1, x_2\} \subseteq C'$. Now, assume that the result is true for $k \in [\![2, n-1]\!]$. Consider $C^1 \in \mathcal{C}'$ such that $\{x_1, \ldots, x_k\} \subseteq C^1$. Since $x_k \prec_{\mathcal{C}'} x_{k+1}$, then $\exists\, C^2 \in \mathcal{C}'$ such that $(x_k, x_{k+1}) \in (C^2)^2$. Analogously, we can show that C^2_1 (illustrated in Figure 3-12), which is in $\mathcal{C}'$, contains $\{x_1, \ldots, x_{k+1}\}$. Therefore, by induction, we obtain that $\exists\, C' \in \mathcal{C}'$ such that $C = \{x_1, \ldots, x_n\} \subseteq C'$. Since $C \subseteq X'$, then we have $C = C \cap X' \subseteq C' \cap X'$.

Now, assume that $\exists\, x' \in C' \cap X' \backslash C$. For every $k \in [\![1, n]\!]$, $(x_k, x') \in (C')^2$. Therefore, x' is comparable in P' with every element of the chain C. This implies that $C \cup \{x'\}$ is a chain in P', which contradicts the maximality of C in P'. Therefore, $C = C' \cap X'$. □

Proof of Proposition 9. First, let us show that the set of constraints (3.1a)-(3.1b) is equivalent to the set of constraints (3.5)-(3.6). Let $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ be a vector that satisfies $\sum_{\{S \in \mathcal{P} \,|\, x \in S\}} \sigma_S = \rho_x, \forall x \in X$. For every maximal chain $C \in \mathcal{C}$, we have the following equality:

$$\sum_{x \in C} \rho_x = \sum_{x \in C} \sum_{\{S \in \mathcal{P} \,|\, x \in S\}} \sigma_S = \sum_{S \in \mathcal{P}} \sigma_S \sum_{x \in C} \mathbb{1}_{\{x \in S\}} = \sum_{\{S \in \mathcal{P} \,|\, S \cap C \neq \emptyset\}} \sigma_S |S \cap C|. \tag{3.23}$$

Therefore, for every maximal chain $C \in \mathcal{C}$, we obtain:

$$\begin{aligned} \sum_{\{S \in \mathcal{P} \,|\, S \cap C \neq \emptyset\}} \sigma_S \geq \pi_C \overset{(3.4),(3.23)}{\iff} \delta_C &\geq \sum_{\{S \in \mathcal{P} \,|\, S \cap C \neq \emptyset\}} \sigma_S (|S \cap C| - 1) \\ &= \sum_{\{S \in \mathcal{P} \,||\, S \cap C| \geq 2\}} \sigma_S (|S \cap C| - 1). \end{aligned} \tag{3.24}$$

Now, let us show that $(\mathcal{D})$ is feasible if and only if the optimal value of $(\mathcal{Q})$ satisfies $z^*_{(\mathcal{Q})} \leq 1$.

– If $\exists\, \sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ that satisfies (3.1a)-(3.1c), then we showed that σ also satisfies

(3.5)-(3.6). Therefore, σ is a feasible solution of $(\mathcal{Q})$. Furthermore, the objective value of σ is equal to 1, which implies that $z^*_{(\mathcal{Q})} \leq 1$.

– If $z^*_{(\mathcal{Q})} \leq 1$, let σ^* be an optimal solution of $(\mathcal{Q})$. Necessarily, $\sigma^*_\emptyset = 0$ and we can define a vector $\sigma \in \mathbb{R}^{|\mathcal{P}|}$ as follows: $\sigma_S = \sigma^*_S$, $\forall S \in \mathcal{P}\backslash\emptyset$, and $\sigma_\emptyset = 1 - \sum_{S\in\mathcal{P}\backslash\emptyset} \sigma^*_S = 1 - z^*_{(\mathcal{Q})} \geq 0$. Therefore, $\sigma \in \mathbb{R}^{|\mathcal{P}|}_+$ and satisfies (3.5)-(3.6), which we showed is equivalent to satisfying (3.1a)-(3.1b). Finally, σ satisfies (3.1c) by construction. Thererefore, σ is feasible for $(\mathcal{D})$.

□

3.6.2 Proofs of Section 3.3

Proof of Proposition 10. We show $(i) - (iv)$ by induction.

First, consider $k = 1$. Since $\mathcal{C}^1 = \mathcal{C}$, $\rho^1 = \rho$, $\pi^1 = \pi$, and $\delta^1 = \delta$, then (i) follows from (3.2) and (3.4). Since $X^0 = X$, and $\mathcal{C}^1 = \mathcal{C}$ contains all maximal chains, then (ii) is automatically satisfied. (iii) is a direct consequence of (3.3).

Now we apply Lemma 10 to show (iv), i.e., $P^1 = (X^1, \preceq_{\overline{\mathcal{C}}^1})$ is a poset. Specifically, we show that $\overline{\mathcal{C}}^1$ preserves the decomposition of maximal chains intersecting in X^1. Consider $C^1, C^2 \in \overline{\mathcal{C}}^1$ such that $C^1 \cap C^2 \cap X^1 \neq \emptyset$, and let us consider the other two maximal chains C^2_1 and C^1_2, which we know from (ii) are in $\mathcal{C}^1$, since $X^1 \subseteq X^0$. We need to show that they are also in $\overline{\mathcal{C}}^1$. Let $x^* \in C^1 \cap C^2 \cap X^1$, and let us rewrite $C^1 = \{x_{-k}, \ldots, x_{-1}, x_0 = x^*, x_1, \ldots, x_n\}$ and $C^2 = \{y_{-l}, \ldots, y_{-1}, y_0 = x^*, y_1, \ldots, y_m\}$. Then, $C^2_1 = \{x_{-k}, \ldots, x_{-1}, x^*, y_1, \ldots, y_m\}$ and $C^1_2 = \{y_{-l}, \ldots, y_{-1}, x^*, x_1, \ldots, x_n\}$. We now use $(i) - (iii)$: Since $C^1, C^2 \in \overline{\mathcal{C}}^1$; the conservation law is satisfied by π^1 on the maximal chains in $\mathcal{C}^1$ intersecting in X^0; $C^2_1, C^1_2 \in \mathcal{C}^1$; and since $\delta^1 \geq 0$ on $\mathcal{C}^1$, we have:

$$\sum_{i=-k}^{n} \rho^1_{x_i} + \sum_{j=-l}^{m} \rho^1_{y_j} = \pi^1_{C^1} + \pi^1_{C^2} = \pi^1_{C^2_1} + \pi^1_{C^1_2} = \sum_{x\in C^2_1} \rho^1_x + \sum_{x\in C^1_2} \rho^1_x - \delta^1_{C^2_1} - \delta^1_{C^1_2}$$
$$\leq \sum_{i=-k}^{n} \rho^1_{x_i} + \sum_{j=-l}^{m} \rho^1_{y_j}.$$

Therefore, $\delta^1_{C_1^2} = \delta^1_{C_2^1} = 0$, and C_1^2 and C_2^1 are in $\overline{\mathcal{C}}^1$. From Lemma 10, we conclude that $P^1 = (X^1, \preceq_{\overline{\mathcal{C}}^1})$ is a poset.

We now assume that $(i) - (iv)$ hold for $k \in [\![1, n^*]\!]$, and show that they also hold for $k+1$:

(i) Since P^k is a poset, the $k-$th iteration of the algorithm is well-defined, and we can consider the set S^k and the weight w^k at that iteration. Then, for every $C \in \mathcal{C}$, (A8), (A9), and (3.7) give us:

$$\begin{aligned}\sum_{x \in C} \rho_x^{k+1} - \pi_C^{k+1} &= \sum_{x \in C} \rho_x^k - \pi_C^k - w^k |C \cap S^k| + w^k \mathbb{1}_{\{S^k \cap C \neq \emptyset\}} \\ &= \delta_C^k - w^k (|C \cap S^k| - 1) \mathbb{1}_{\{S^k \cap C \neq \emptyset\}} = \delta_C^{k+1}.\end{aligned}$$

Now, consider a maximal chain $C \in \mathcal{C}^k$. Since $\delta^k \geq 0$ on $\mathcal{C}^k$, then $\mathcal{C}^k = \overline{\mathcal{C}}^k \cup \widehat{\mathcal{C}}^k$ (from (A12)).

(a) If $C \in \overline{\mathcal{C}}^k$, then by definition of $\preceq_{\overline{\mathcal{C}}^k}$, $C \cap X^k$ is a chain in P^k. From Lemma 9, we know that S^k is an antichain of P^k. Therefore, $|S^k \cap (C \cap X^k)| \leq 1$. Since $S^k \subseteq X^k$, we obtain that $|S^k \cap C| = |(S^k \cap X^k) \cap C| = |S^k \cap (C \cap X^k)| \leq 1$. Thus:

$$\delta_C^{k+1} \overset{\text{(A9)}}{=} \delta_C^k - w^k (|C \cap S^k| - 1) \mathbb{1}_{\{|S^k \cap C| \geq 2\}} = \delta_C^k = 0.$$

(b) If $C \in \widehat{\mathcal{C}}^k$, then by definition of w^k, we have:

$$\delta_C^{k+1} \overset{\text{(A9)}}{=} \delta_C^k - w^k (|S^k \cap C| - 1) \mathbb{1}_{\{|S^k \cap C| \geq 2\}} \overset{\text{(A7)}}{\geq} 0.$$

In summary, for all $C \in \mathcal{C}^k$, $\delta_C^{k+1} \geq 0$. Since $\mathcal{C}^{k+1} \overset{\text{(A10)}}{\subseteq} \mathcal{C}^k$, then for all $C \in \mathcal{C}^{k+1}$, $\delta_C^{k+1} \geq 0$.

(ii) Consider $C^1, C^2 \in \mathcal{C}^{k+1} \subseteq \mathcal{C}^k$ such that $C^1 \cap C^2 \cap X^k \neq \emptyset$, and let C_1^2 and C_2^1 be the other two maximal chains such that $C_1^2 \cup C_2^1 = C^1 \cup C^2$. Since $X^k \overset{\text{(A11)}}{\subseteq} X^{k-1}$, then $C^1 \cap C^2 \cap X^{k-1} \neq \emptyset$. Therefore, by inductive hypothesis, C_1^2, $C_2^1 \in \mathcal{C}^k$ as well. Let x_1 (resp. y_1) denote the minimal element of the chain

$C^1 \cap X^k$ (resp. $C^2 \cap X^k$) in P. Since C^1, $C^2 \in \mathcal{C}^{k+1}$, then $(x_1, y_1) \overset{(A10)}{\in} (S^k)^2$. Let $x^* \in X^k$ denote an intersecting point of C^1 and C^2. Since $C^1 \cap X^k$ is a chain in P, contains x^*, and whose minimal element is x_1, then necessarily, $x_1 \preceq x^*$. Similarly, we obtain that $y_1 \preceq x^*$. Therefore, the minimal element of $C_1^2 \cap X^k$ (resp. $C_2^1 \cap X^k$) is x_1 (resp. y_1), which is in S^k. Thus, $C_1^2, C_2^1 \in \mathcal{C}^{k+1}$, and $\mathcal{C}^{k+1}$ preserves the decomposition of maximal chains of P intersecting in X^k.

(iii) Now, given C^1, C^2 in $\mathcal{C}^{k+1}$ that intersect in X^k, we just proved that C_1^2 and C_2^1 are in $\mathcal{C}^{k+1}$ as well. Therefore, $\forall C \in \{C^1, C^2, C_1^2, C_2^1\}$, we have $\pi_C^{k+1} \overset{(3.7)}{=} \pi_C^k - w^k$ (since $S^k \cap C \neq \emptyset$). By inductive hypothesis, since $\mathcal{C}^{k+1} \subseteq \mathcal{C}^k$ and $X^{k+1} \subseteq X^k$, π^k satisfies the conservation law between C^1, C^2, C_1^2, and C_2^1. Thus, we can conclude that:

$$\pi_{C^1}^{k+1} + \pi_{C^2}^{k+1} = \pi_{C^1}^k + \pi_{C^2}^k - 2w^k = \pi_{C_1^2}^k + \pi_{C_2^1}^k - 2w^k = \pi_{C_1^2}^{k+1} + \pi_{C_2^1}^{k+1}.$$

(iv) This is a consequence of $(i) - (iii)$; the proof is analogous to the one derived for the first step of the induction.

Therefore, we conclude by induction that $(i) - (iv)$ hold for every $k \in [\![1, n^* + 1]\!]$.

□

Proof of Lemma 11. Consider $C^{(1)} \in \mathcal{C}$, and suppose that $\exists\, k_1 \in [\![1, n^*]\!]$ such that $C^{(1)} \in \mathcal{C}^{k_1}$, $C^{(1)} \cap X^{k_1} \neq \emptyset$, but $C^{(1)} \notin \mathcal{C}^{k_1+1}$. This case arises when the minimal element of $C^{(1)} \cap X^{k_1}$ in P is not a minimal element of P^{k_1}. Then, we can find a chain in P^{k_1} whose maximal element is the minimal element of $C^{(1)} \cap X^{k_1}$ in P, and whose minimal element is a minimal element of P^{k_1}. From the definition of P^{k_1} and Lemma 10, this chain is contained in a maximal chain in $\overline{\mathcal{C}}^{k_1}$. We can then exploit $(i) - (iii)$ in Proposition 10 to show that there exists a maximal chain in $\mathcal{C}^{k_1+1}$ that satisfies the desired properties.

Formally, let x^* denote the minimal element of $C^{(1)} \cap X^{k_1}$ in P. Since $C^{(1)} \notin \mathcal{C}^{k_1+1}$, then $x^* \notin S^{k_1}$, i.e., x^* is not a minimal element of P^{k_1}. Let $C' \subseteq X^{k_1}$ denote a maximal chain of P^{k_1} that contains x^*. From Lemma 9, we know that the minimal element of

C' in P^{k_1}, which we denote y_1, is a minimal element of P^{k_1}. Therefore $y_1 \in S^k$ and $y_1 \neq x^*$. Thus, C' is of size at least two, and there exists a maximal chain $C^2 \in \overline{\mathcal{C}}^{k_1}$ such that $C' = C^2 \cap X^{k_1}$ (Lemma 10). Since $C^{(1)} \cap C^2 \cap X^{k_1 - 1} \supseteq \{x^*\} \neq \emptyset$, let us consider the other two maximal chains $C_1^2, C_2^1 \in \mathcal{C}$ such that $C_1^2 \cup C_2^1 = C^{(1)} \cup C^2$. Since $C^{(1)}$ and C^2 are in $\mathcal{C}^{k_1}$, then from Proposition 10, C_1^2 and C_2^1 are in $\mathcal{C}^{k_1}$ as well. Let us rewrite:

$$C^{(1)} = \{x_{-m}, \dots, x_0 = x^*, \dots, x_n\}, \quad C^2 = \{y_{-q}, \dots, y_0, y_1, \dots, y_p = x^*, \dots, y_{p+r}\},$$
$$C_1^2 = \{x_{-m}, \dots, x_{-1}, y_p, \dots, y_{p+r}\}, \quad C_2^1 = \{y_{-q}, \dots, y_p, x_1, \dots, x_n\};$$

they are illustrated in Figure 3-13.

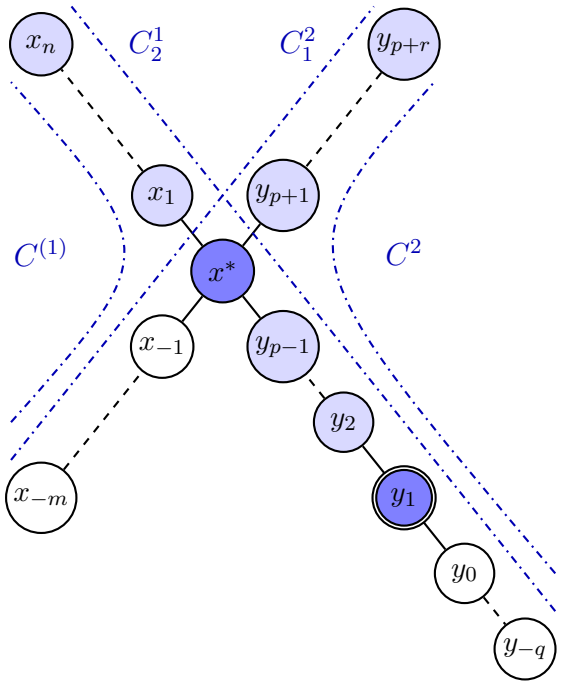


Figure 3-13: Illustration of $C^{(1)}$, C^2, C_1^2, and C_2^1. In dark blue are the elements in X^{k_1}, in light blue are the elements that may or may not be in X^{k_1}, and in white are the elements that are not in X^{k_1}. The "double" node y_1 is in S^{k_1}.

Since x^* is the minimal element of $C^{(1)} \cap X^{k_1}$ in P, then $\forall i \in [\![-m, -1]\!]$, $x_i \notin X^{k_1}$ and $\rho_{x_i}^{k_1} = 0$. Since $C^2 \in \overline{\mathcal{C}}^{k_1}$ and $C_1^2 \in \mathcal{C}^{k_1}$, and from the conservation law between

$C^{(1)}$, C^2, C_1^2 and C_2^1, we obtain:

$$\pi_{C_2^1}^{k_1} - \pi_{C^{(1)}}^{k_1} \overset{(3.10)}{=} \pi_{C^2}^{k_1} - \pi_{C_1^2}^{k_1} \overset{(3.8)}{=} \sum_{j=-q}^{p+r} \rho_{y_j}^{k_1} - \underbrace{\delta_{C^2}^{k_1}}_{=0} - \sum_{i=-m}^{-1} \underbrace{\rho_{x_i}^{k_1}}_{=0} - \sum_{j=p}^{p+r} \rho_{y_j}^{k_1} + \underbrace{\delta_{C_1^2}^{k_1}}_{\geq 0}$$
$$\overset{(3.9)}{\geq} \sum_{j=-q}^{p-1} \rho_{y_j}^{k_1}. \tag{3.25}$$

This implies that:

$$\delta_{C^{(1)}}^{k_1} \overset{(3.8)}{=} \sum_{i=0}^{n} \rho_{x_i}^{k_1} - \pi_{C^{(1)}}^{k_1} + \sum_{j=-q}^{p-1} \rho_{y_j}^{k_1} - \sum_{j=-q}^{p-1} \rho_{y_j}^{k_1} \overset{(3.8)}{=} \delta_{C_2^1}^{k_1} + \pi_{C_2^1}^{k_1} - \pi_{C^{(1)}}^{k_1} - \sum_{j=-q}^{p-1} \rho_{y_j}^{k_1}$$
$$\overset{(3.25)}{\geq} \delta_{C_2^1}^{k_1}.$$

Furthermore, since y_1 is the minimal element of $C^2 \cap X^{k_1}$ in P^{k_1}, it is also the minimal element of $C^2 \cap X^{k_1}$ in P. This implies that y_1 is the minimal element of $C_2^1 \cap X^{k_1}$ in P. Since y_1 belongs to S^{k_1}, we deduce that $C_2^1 \in \mathcal{C}^{k_1+1}$.

Finally, since $\forall i \in [\![-m, -1]\!]$, $x_i \notin X^{k_1}$, then $C_2^1 \cap X^{k_1} \supseteq \{x^*, x_1, \ldots, x_n\} \cap X^{k_1} = C^{(1)} \cap X^{k_1}$, as illustrated in Figure 3-13. In conclusion, given $C^{(1)} \in \mathcal{C}^{k_1} \backslash \mathcal{C}^{k_1+1}$ such that $C^{(1)} \cap X^{k_1} \neq \emptyset$, $\exists\, C^{(2)} \coloneqq C_2^1 \in \mathcal{C}^{k_1+1}$ such that $\delta_{C^{(1)}}^{k_1} \geq \delta_{C^{(2)}}^{k_1}$ and $C^{(2)} \cap X^{k_1} \supseteq C^{(1)} \cap X^{k_1}$. □

Proof of Proposition 11. We recall that the algorithm terminates after iteration n^* if $X^{n^*+1} = \emptyset$. First, we note that $X^1 \subseteq X$ and $\forall k \in [\![1, n^*]\!]$, $X^{k+1} \overset{(A11)}{\subseteq} X^k$. Additionally, $\widehat{\mathcal{C}}^1 \subseteq \mathcal{C}$, and from (A9), we have $\forall k \in [\![1, n^*]\!]$, $\widehat{\mathcal{C}}^{k+1} \subseteq \widehat{\mathcal{C}}^k$. Now, consider $k \in [\![1, n^*]\!]$, and the weight w^k chosen by the algorithm at iteration k. From (A7), $\exists\, x \in X^k$ such that $w^k = \rho_x^k$, or $\exists\, C \in \widehat{\mathcal{C}}^k$ such that $w^k = \frac{\delta_C^k}{|S^k \cap C| - 1}$. In the first case, we deduce that $x \notin X^{k+1}$, so $X^{k+1} \subsetneq X^k$. In the second case, either $C \notin \mathcal{C}^{k+1}$, or $C \in \mathcal{C}^{k+1}$ and $\delta_C^{k+1} = 0$, which both imply that $C \in \overline{\mathcal{C}}^{k+1}$. Therefore, $C \notin \widehat{\mathcal{C}}^{k+1}$ and $\widehat{\mathcal{C}}^{k+1} \subsetneq \widehat{\mathcal{C}}^k$.

Thus, $\forall k \in [\![1, n^*]\!]$, $|X^{k+1} \times \widehat{\mathcal{C}}^{k+1}| < |X^k \times \widehat{\mathcal{C}}^k|$. Since $|X^1 \times \widehat{\mathcal{C}}^1| \in \mathbb{N}$, if n^* were equal to $+\infty$, we would obtain an infinite decreasing sequence of natural integers. Therefore, we conclude that $n^* \in \mathbb{N}$, i.e., the algorithm terminates. At termination,

we have $X^{n^*+1} = \emptyset$.

Next, we show that the output $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ of the algorithm is a feasible solution of $(\mathcal{Q})$. First, the equality constraints (3.5) are trivially satisfied:

$$\forall x \in X,\ \rho_x \overset{\text{(A1)}}{=} \rho_x^1 \overset{\text{(A8)}}{=} \underbrace{\rho_x^{n^*+1}}_{=0} + \sum_{k=1}^{n^*} w^k \mathbb{1}_{\{x \in S^k\}} \overset{\text{(A7)}}{=} \sum_{k=1}^{n^*} \sigma_{S^k} \mathbb{1}_{\{x \in S^k\}} = \sum_{\{S \in \mathcal{P} \,|\, x \in S\}} \sigma_S.$$

Regarding constraints (3.6), we first show the following equality:

$$\begin{aligned}\forall C \in \mathcal{C},\ \delta_C^{n^*+1} &\overset{\text{(A9)}}{=} \delta_C^1 - \sum_{k=1}^{n^*} w^k (|S^k \cap C| - 1) \mathbb{1}_{\{|S^k \cap C| \geq 2\}} \\ &\overset{\text{(A1)},\text{(A7)}}{=} \delta_C - \sum_{\{S \in \mathcal{P} \,|\, |S \cap C| \geq 2\}} \sigma_S (|S \cap C| - 1).\end{aligned}$$

Therefore, constraints (3.6) are satisfied if and only if $\forall C \in \mathcal{C},\ \delta_C^{n^*+1} \geq 0$.

From Proposition 10, we know that $\forall C \in \mathcal{C}^{n^*+1},\ \delta_C^{n^*+1} \geq 0$. Now, consider $C^{(1)} \in \mathcal{C}$, and suppose that $\exists\, k_1 \in [\![1, n^*]\!]$ such that $C^{(1)} \in \mathcal{C}^{k_1} \backslash \mathcal{C}^{k_1+1}$.

- If $C^{(1)} \cap X^{k_1} = \emptyset$, then $\forall l \in [\![k_1, n^*]\!],\ |S^l \cap C^{(1)}| = 0$ since $S^l \overset{\text{(A6)}}{\subseteq} X^l$ and $X^l \overset{\text{(A11)}}{\subseteq} X^{k_1}$. Therefore, since $C^{(1)} \in \mathcal{C}^{k_1}$, we have:

$$\delta_{C^{(1)}}^{n^*+1} \overset{\text{(A9)}}{=} \delta_{C^{(1)}}^{k_1} - \sum_{l=k_1}^{n^*} w^l (|S^l \cap C^{(1)}| - 1) \mathbb{1}_{\{|S^l \cap C^{(1)}| \geq 2\}} = \delta_{C^{(1)}}^{k_1} \overset{(3.9)}{\geq} 0.$$

- If $C^{(1)} \cap X^{k_1} \neq \emptyset$, then $\exists\, C^{(2)} \in \mathcal{C}^{k_1+1}$ such that $\delta_{C^{(1)}}^{k_1} \geq \delta_{C^{(2)}}^{k_1}$ and $C^{(2)} \cap X^{k_1} \supseteq C^{(1)} \cap X^{k_1}$ (Lemma 11). Consider $i \in [\![k_1, n^*]\!]$. Since $S^i \overset{\text{(A6)},\text{(A11)}}{\subseteq} X^{k_1}$, then $S^i \cap C^{(2)} \supseteq S^i \cap C^{(1)}$, and we obtain:

$$\begin{aligned}\forall l \in [\![k_1, n^*+1]\!],\ \delta_{C^{(1)}}^l &\overset{\text{(A9)}}{=} \delta_{C^{(1)}}^{k_1} - \sum_{i=k_1}^{l-1} w^i (|S^i \cap C^{(1)}| - 1) \mathbb{1}_{\{|S^i \cap C^{(1)}| \geq 2\}} \\ &\geq \delta_{C^{(2)}}^{k_1} - \sum_{i=k_1}^{l-1} w^i (|S^i \cap C^{(2)}| - 1) \mathbb{1}_{\{|S^i \cap C^{(2)}| \geq 2\}} \\ &\overset{\text{(A9)}}{=} \delta_{C^{(2)}}^l. \end{aligned} \tag{3.26}$$

In particular, $\delta^{n^*+1}_{C^{(1)}} \geq \delta^{n^*+1}_{C^{(2)}}$. We note that $C^{(2)} \in \mathcal{C}^{k_1+1}$, and two cases can arise:

1) $C^{(2)} \in \mathcal{C}^{n^*+1}$. In this case, $\delta^{n^*+1}_{C^{(2)}} \geq 0$ (Proposition 10).

2) $\exists\, k_2 \in [\![k_1+1, n^*]\!]$ such that $C^{(2)} \in \mathcal{C}^{k_2} \backslash \mathcal{C}^{k_2+1}$. Then we reiterate the same argument:

   (a) If $C^{(2)} \cap X^{k_2} = \emptyset$, then $\delta^{n^*+1}_{C^{(2)}} = \delta^{k_2}_{C^{(2)}} \overset{(3.9)}{\geq} 0$.

   (b) If $C^{(2)} \cap X^{k_2} \neq \emptyset$, then there exists $C^{(3)} \in \mathcal{C}^{k_2+1}$ such that $\delta^{k_2}_{C^{(2)}} \geq \delta^{k_2}_{C^{(3)}}$ and $C^{(3)} \cap X^{k_2} \supseteq C^{(2)} \cap X^{k_2}$ (Lemma 11). Analogous calculations to (3.26) show that $\delta^{n^*+1}_{C^{(2)}} \geq \delta^{n^*+1}_{C^{(3)}}$.

By induction, we construct a sequence of maximal chains $(C^{(s)})$, a sequence of increasing integers (k_s), and a termination point $s^* \in \mathbb{N}^*$, such that:

$$\forall s \in [\![1, s^*-1]\!],\ C^{(s)} \in \mathcal{C}^{k_s} \backslash \mathcal{C}^{k_s+1},\ \delta^{n^*+1}_{C^{(s)}} \geq \delta^{n^*+1}_{C^{(s+1)}},\ \text{and } \delta^{n^*+1}_{C^{(s^*)}} \geq 0.$$

Note that s^* exists since $k_s \leq n^*+1$. Then, we deduce that $\delta^{n^*+1}_{C^{(1)}} \geq \cdots \geq \delta^{n^*+1}_{C^{(s^*)}} \geq 0$.

Thus, $\forall C \in \mathcal{C},\ \delta^{n^*+1}_C \geq 0$, and constraints (3.6) are satisfied by the output σ of the algorithm. In conclusion, the algorithm outputs a feasible solution of $(\mathcal{Q})$. □

Proof of Proposition 12. For all $k \in [\![1, n^*+1]\!]$, let $W^k \coloneqq \max\{\max\{\rho^k_x,\ x \in X\}, \max\{\pi^k_C,\ C \in \mathcal{C}\}\}$. First, we show that $\forall k \in [\![1, n^*]\!]$, $W^{k+1} = W^k - w^k$. Consider $k \in [\![1, n^*]\!]$, and let $C \in \mathcal{C} \backslash \mathcal{C}^{k+1}$. Then, there exists $k_1 \leq k$ such that $C \in \mathcal{C}^{k_1} \backslash \mathcal{C}^{k_1+1}$.

– If $C \cap X^{k_1} = \emptyset$, then $\pi^{k+1}_C \leq \pi^k_C \leq \pi^{k_1}_C \overset{(3.8)}{=} -\delta^{k_1}_C \overset{(3.9)}{\leq} 0$.

– If $C \cap X^{k_1} \neq \emptyset$, then $\exists\, C^{(2)} \in \mathcal{C}^{k_1+1}$ such that $\delta^{k_1}_C \geq \delta^{k_1}_{C^{(2)}}$ and $C^{(2)} \cap X^{k_1} \supseteq C \cap X^{k_1}$ (Lemma 11). This implies that $\forall l \in [\![k_1, n^*+1]\!]$, $\delta^l_C \overset{(3.26)}{\geq} \delta^l_{C^{(2)}}$, and

$C^{(2)} \cap X^l \supseteq C \cap X^l$. Then, we obtain:

$$\begin{aligned}\forall l \in [\![k_1, n^* + 1]\!],\ \pi_C^l &\overset{(3.8)}{=} \sum_{x \in C \cap X^l} \rho_x^l - \delta_C^l + \pi_{C^{(2)}}^l + \delta_{C^{(2)}}^l \\ &\quad - \sum_{x \in C \cap X^l} \rho_x^l - \sum_{x \in (C^{(2)} \cap X^l) \setminus (C \cap X^l)} \rho_x^l \\ &\overset{(3.26)}{\leq} \pi_{C^{(2)}}^l.\end{aligned}$$

In particular, we deduce that $\pi_C^k \leq \pi_{C^{(2)}}^k$ and $\pi_C^{k+1} \leq \pi_{C^{(2)}}^{k+1}$.

As in Proposition 11, we construct a sequence of maximal chains $(C^{(s)})$, a sequence of increasing integers (k_s), and a termination point $s' \in \mathbb{N}^*$, such that:

$$C^{(1)} = C, \quad \forall s \in [\![1, s' - 1]\!],\ C^{(s)} \in \mathcal{C}^{k_s} \setminus \mathcal{C}^{k_s+1},\ \pi_{C^{(s)}}^k \leq \pi_{C^{(s+1)}}^k, \text{ and } \pi_{C^{(s)}}^{k+1} \leq \pi_{C^{(s+1)}}^{k+1}.$$

At termination, $C^{(s')} \in \mathcal{C}^{k_{s'}}$, and either $k_{s'} = k+1$, or $k_{s'} < k+1$ and $C^{(s')} \cap X^{k_{s'}} = \emptyset$.

- If $k_{s'} = k + 1$, then we conclude that $\pi_C^k \leq \pi_{C^{(s')}}^k$ and $\pi_C^{k+1} \leq \pi_{C^{(s')}}^{k+1}$, with $C^{(s')} \in \mathcal{C}^{k+1}$.

- If $k_{s'} < k + 1$ and $C^{(s')} \cap X^{k_{s'}} = \emptyset$, then:

$$\pi_C^{k+1} \overset{(3.7)}{\leq} \pi_C^k \leq \pi_{C^{(s')}}^k \overset{(3.7)}{\leq} \pi_{C^{(s')}}^{k_{s'}} \overset{(3.8)}{=} -\delta_{C^{(s')}}^{k_{s'}} \overset{(3.9)}{\leq} 0 \leq \rho_x^{k+1} \overset{(8)}{\leq} \rho_x^k,\ \forall x \in X.$$

Thus, we deduce that $W^k = \max\{\max\{\rho_x^k,\ x \in X\}, \max\{\pi_C^k,\ C \in \mathcal{C}^{k+1}\}\}$, and $W^{k+1} = \max\{\max\{\rho_x^{k+1},\ x \in X\}, \max\{\pi_C^{k+1},\ C \in \mathcal{C}^{k+1}\}\}$.

Since $k \in [\![1, n^*]\!]$ and Algorithm 1 terminates after the n^*-th iteration, we know that $X^k \neq \emptyset$. Furthermore, since $\forall x \in X^k,\ \rho_x^k \geq \rho_x^{k+1} \geq 0$, and $\forall x \in X \setminus X^k$, $\rho_x^k = \rho_x^{k+1} = 0$, then $\max\{\rho_x^k,\ x \in X\} = \max\{\rho_x^k,\ x \in X^k\}$, and $\max\{\rho_x^{k+1},\ x \in X\} = \max\{\rho_x^{k+1},\ x \in X^k\}$.

Next, we consider $x \in X^k \setminus S^k$. Then, $\exists\, y \neq x \in X^k$ such that $y \preceq_{\overline{\mathcal{C}}^k} x$, and $y \in S^k$ is a minimal element in P^k. By definition, $\exists\, C \in \overline{\mathcal{C}}^k$ such that $y, x \in C$, and

$y \prec x$. In fact, y is the minimal element of $C \cap X^k$ in P^k, and $C \in \mathcal{C}^{k+1}$. Since $C \in \overline{\mathcal{C}}^k$, then $\pi_C^k \overset{(3.8)}{=} \sum_{x' \in C} \rho_{x'}^k \geq \rho_x^k + \rho_y^k \geq \rho_x^k$. Furthermore, since $y \in S^k$, then $w^k \overset{(A7)}{\leq} \rho_y^k$. Thus, we obtain that $\rho_x^{k+1} = \rho_x^k \leq \pi_C^k - \rho_y^k \leq \pi_C^k - w^k \overset{(3.7)}{=} \pi_C^{k+1}$, from which we conclude that $W^k = \max\{\max\{\rho_x^k,\ x \in S^k\}, \max\{\pi_C^k,\ C \in \mathcal{C}^{k+1}\}\}$, and $W^{k+1} = \max\{\max\{\rho_x^{k+1},\ x \in S^k\}, \max\{\pi_C^{k+1},\ C \in \mathcal{C}^{k+1}\}\}$.

Finally, we note that $\forall C \in \mathcal{C}^{k+1}$, $\pi_C^{k+1} \overset{(3.7)}{=} \pi_C^k - w^k$ since $S^k \cap C \neq \emptyset$, and $\forall x \in S^k$, $\rho_x^{k+1} \overset{(A8)}{=} \rho_x^k - w^k$. Putting everything together, we conclude:

$$\begin{aligned} W^{k+1} &= \max\{\max\{\rho_x^{k+1},\ x \in S^k\}, \max\{\pi_C^{k+1},\ C \in \mathcal{C}^{k+1}\}\} \\ &= \max\{\max\{\rho_x^k,\ x \in S^k\}, \max\{\pi_C^k,\ C \in \mathcal{C}^{k+1}\}\} - w^k = W^k - w^k. \end{aligned}$$

Next, we show that $W^{n^*+1} = 0$. First, we know that $\forall x \in X$, $\rho_x^{n^*+1} = 0$. Secondly, $\forall C \in \mathcal{C}^{n^*+1}$, we have $\pi_C^{n^*+1} \overset{(3.8)}{=} -\delta_C^{n^*+1} \overset{(3.9)}{\leq} 0$. Thirdly, $S^{n^*} \neq \emptyset$ since P^{n^*} is a nonempty poset. This implies that:

$$W^{n^*+1} = \max\{\max\{\rho_x^{n^*+1},\ x \in S^{n^*}\}, \max\{\pi_C^{n^*+1},\ C \in \mathcal{C}^{n^*+1}\}\} = 0.$$

Finally, using a telescoping series, we obtain:

$$\begin{aligned} \sum_{S \in \mathcal{P}} \sigma_S &\overset{(A7)}{=} \sum_{k=1}^{n^*} w^k = \sum_{k=1}^{n^*} W^k - W^{k+1} = W^1 - \underbrace{W^{n^*+1}}_{=0} \\ &\overset{(A1),(3.7)}{=} \max\{\max\{\rho_x,\ x \in X\}, \max\{\pi_C,\ C \in \mathcal{C}\}\}. \end{aligned}$$

□

3.6.3 Proofs of Section 3.4

Proof of Lemma 12. Let $z^*_{(\mathcal{M}')}$ denote the optimal value of $(\mathcal{M}'_P)$ and $(\mathcal{M}'_D)$, and let $f^* \in \mathbb{R}_+^{|\Lambda|}$ be an optimal solution of $(\mathcal{M}_P)$. Then, $f' \in \mathbb{R}_+^{|\mathcal{E}|}$ defined by $f'_{ij} =$

$\sum_{\{\lambda\in\Lambda\,|\,(i,j)\in\lambda\}} f^*_\lambda$ is a feasible solution of $(\mathcal{M}'_P)$. Therefore:

$$z^*_{(\mathcal{M}')} \geq \sum_{\{i\in\mathcal{V}\,|\,(i,t)\in\mathcal{E}\}} f'_{it} - \sum_{(i,j)\in\mathcal{E}} \frac{b_{ij}}{p_1} f'_{ij} = \sum_{\lambda\in\Lambda} \pi^0_\lambda f^*_\lambda = z^*_{(\mathcal{M})}.$$

Now, let $f' \in \mathbb{R}_+^{|\mathcal{E}|}$ be an optimal solution of $(\mathcal{M}'_P)$. From the flow decomposition theorem, there exists a vector $f^* \in \mathbb{R}_+^{|\Lambda|}$ such that $\forall (i,j) \in \mathcal{E},\ f'_{ij} = \sum_{\{\lambda\in\Lambda\,|\,(i,j)\in\lambda\}} f^*_\lambda$. Since f^* is a feasible solution of $(\mathcal{M}_P)$, we deduce that $z^*_{(\mathcal{M})} \geq z^*_{(\mathcal{M}')}$. In conclusion, $z^*_{(\mathcal{M})} = z^*_{(\mathcal{M}')}$, and an optimal solution of $(\mathcal{M}_P)$ can be obtained by decomposing an optimal solution of $(\mathcal{M}'_P)$ into $s-t$ paths.

Now, consider an optimal solution (ρ', μ', y') of $(\mathcal{M}'_D)$. Then, one can verify that for every $s-t$ path $\lambda \in \Lambda$:

$$\sum_{(i,j)\in\lambda} (\rho'_{ij} + \mu'_{ij}) \geq 1 - \frac{1}{p_1} \sum_{(i,j)\in\lambda} b_{ij} = \pi^0_\lambda,$$

since the y' cancel in a telescopic manner along each $s-t$ path. Therefore, (ρ', μ') is a feasible solution of $(\mathcal{M}_D)$. Since $z^*_{(\mathcal{M}')} = z^*_{(\mathcal{M})}$, we can conclude that (ρ', μ') is an optimal solution of $(\mathcal{M}_D)$. □

Proof of Lemma 13. Let us show that $\preceq_\mathcal{G}$ is a partial order on $\mathcal{E}$.

- Reflexivity: For every $u \in \mathcal{E}$, $u \preceq_\mathcal{G} u$ by definition.

- Antisymmetry: Consider $(u, v) \in \mathcal{E}^2$ such that $u \preceq_\mathcal{G} v$ and $v \preceq_\mathcal{G} u$. If $u \neq v$, then there exists λ^1 and λ^2 in Λ such that λ^1 traverses u and v in this order, and λ^2 traverses v and u in this order. They can be written as follows:

$$\lambda^1 = \{u_1, \ldots, u_n, u, u_{n+1}, \ldots, u_{n+m}, v, u_{n+m+1}, \ldots, u_{n+m+p}\},$$
$$\lambda^2 = \{v_1, \ldots, v_q, v, v_{q+1}, \ldots, v_{q+r}, u, v_{q+r+1}, \ldots, v_{q+r+s}\}.$$

  Then, $\{u, u_{n+1}, \ldots, u_{n+m}, v,\ v_{q+1}, \ldots, v_{q+r}\}$ is a cycle (see Figure 3-14), which contradicts $\mathcal{G}$ being acyclic. Therefore $u = v$.

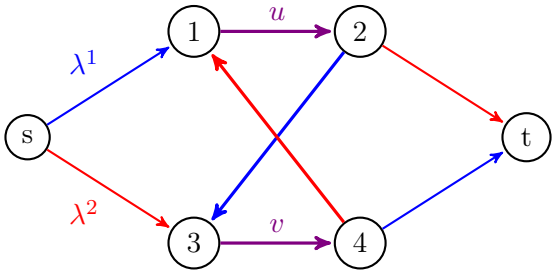


Figure 3-14: Proof of antisymmetry of $\preceq_{\mathcal{G}}$ by contradiction: if $u \preceq_{\mathcal{G}} v$, $v \preceq_{\mathcal{G}} u$, and $u \neq v$, then one can see that u and v necessarily belong to a cycle (shown in thick edges), although $\mathcal{G}$ is acyclic.

– Transitivity: Consider $(u, v, w) \in \mathcal{E}^3$, and assume that $u \preceq_{\mathcal{G}} v$ and $v \preceq_{\mathcal{G}} w$. If $u = v$ or $v = w$, then we trivially obtain that $u \preceq_{\mathcal{G}} w$. Now, let us assume that $u \neq v$ and $v \neq w$. Then, there exists λ^1 and λ^2 in Λ such that λ^1 traverses u and v in this order, and λ^2 traverses v and w in this order. They can be written as follows:

$$\lambda^1 = \{u_1, \ldots, u_n, u, u_{n+1}, \ldots, u_{n+m}, v, u_{n+m+1}, \ldots, u_{n+m+p}\},$$
$$\lambda^2 = \{v_1, \ldots, v_q, v, v_{q+1}, \ldots, v_{q+r}, w, v_{q+r+1}, \ldots, v_{q+r+s}\}.$$

Then, $\lambda_1^2 = \{u_1, \ldots, u_n, u, u_{n+1}, \ldots, u_{n+m}, v, v_{q+1}, \ldots, v_{q+r}, w, v_{q+r+1}, \ldots, v_{q+r+s}\}$ is an $s-t$ path (see Figure 3-15), and traverses u and w in this order. Therefore, $u \preceq_{\mathcal{G}} w$.

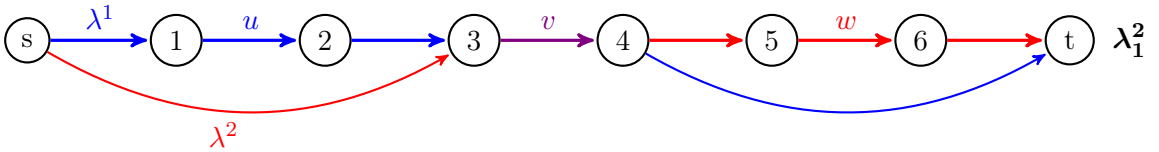


Figure 3-15: Proof of transitivity of $\preceq_{\mathcal{G}}$: if $u \preceq_{\mathcal{G}} v$, and $v \preceq_{\mathcal{G}} w$, then one can construct an $s-t$ path λ_1^2 (in thick line) that traverses u and w in this order.

In conclusion, $P = (\mathcal{E}, \preceq_{\mathcal{G}})$ is a poset.

Next, we prove that the set of maximal chains $\mathcal{C}$ of P is Λ. First, we show that $\mathcal{C} \subseteq \Lambda$. Consider a maximal chain $C \in \mathcal{C}$ of P. If $C = \{u\}$ is of size 1, then necessarily $u = (s, t)$, because $\mathcal{G}$ is connected. Therefore, $C = \{u\}$ is an $s-t$ path. Now, assume

that $|C| \geq 2$. Let us write $C = \{u_1, \ldots, u_n\}$, where $\forall k \in [\![1, n-1]\!],\ u_k \prec_{\mathcal{G}} u_{k+1}$. Since $u_1 \prec_{\mathcal{G}} u_2$ and $u_2 \prec_{\mathcal{G}} u_3$, then there exist λ^1 and λ^2 in Λ such that λ^1 traverses u_1 and u_2 in this order, and λ^2 traverses u_2 and u_3 in this order. When showing the transitivity of $\preceq_{\mathcal{G}}$ in the proof of Lemma 13, we deduced that there exists $\lambda_1^2 \in \Lambda$ that traverses u_1, u_2, and u_3 in this order. If we repeat this process, we obtain an $s-t$ path $\lambda \in \Lambda$ such that $C \subseteq \lambda$.

Now, assume that $\exists\, u \in \lambda \backslash C$. Since $C \subseteq \lambda$, and $u \in \lambda$, then we deduce (by definition of $\preceq_{\mathcal{G}}$) that u is comparable with every element of C. Therefore $C \cup \{u\}$ is a chain in P, which contradicts the maximality of C. Therefore $C = \lambda$ and $\mathcal{C} \subseteq \Lambda$.

To show the reversed inclusion, consider an $s-t$ path $\lambda \in \Lambda$. From the definition of $\preceq_{\mathcal{G}}$, λ is a chain in P. Let us assume that λ is not a maximal chain of P, i.e., there exists a maximal chain $C \in \mathcal{C}$ such that $\lambda \subsetneq C$. Let us write $\lambda = \{u_1, \ldots, u_n\}$ where $\forall k \in [\![1, n-1]\!]$, $u_k \prec_{\mathcal{G}} u_{k+1}$, and let $v \in C \backslash \lambda$. Since $\lambda \subset C$ and $v \in C$, then v is comparable with every element of λ. By transitivity of $\preceq_{\mathcal{G}}$, if $\exists\, k \in [\![1, n]\!]$ such that $v \prec_{\mathcal{G}} u_k$, then $\forall l \in [\![k, n]\!]$, $v \prec_{\mathcal{G}} u_l$. Similarly, if $\exists\, k \in [\![1, n]\!]$ such that $u_k \prec_{\mathcal{G}} v$, then $\forall l \in [\![1, k]\!]$, $u_l \prec_{\mathcal{G}} v$. Therefore, three cases can arise:

- $v \prec_{\mathcal{G}} u_1$. In this case, $\exists\, \lambda^1 = \{w_1, \ldots, w_n, v, w_{n+1}, \ldots, w_{n+m}, u_1, w_{n+m+1}, \ldots, w_{n+m+p}\} \in \Lambda$. However, since λ is an $s-t$ path, then the start node of u_1 is s, which is also the start node of w_1. Therefore, $\{w_1, \ldots, w_n, v, w_{n+1}, \ldots, w_{n+m}\}$ is a cycle, which is a contradiction.

- $u_n \prec_{\mathcal{G}} v$. In this case, $\exists\, \lambda^1 = \{v_1, \ldots, v_q, u_n, v_{q+1}, \ldots, v_{q+r}, v, v_{q+r+1}, \ldots, v_{q+r+s}\} \in \Lambda$. Analogously, we deduce that the end nodes of u_n and v_{q+r+s} are the destination node t, which implies that $\{v_{q+1}, \ldots, v_{q+r}, v, v_{q+r+1}, \ldots, v_{q+r+s}\}$ is a cycle in the acyclic graph $\mathcal{G}$.

- $u_k \prec_{\mathcal{G}} v \prec_{\mathcal{G}} u_{k+1}$ for $k \in [\![1, n-1]\!]$. In this case, there exist two $s-t$ paths $\lambda^1, \lambda^2 \in \Lambda$ defined by:

$$\lambda^1 = \{v_1, \ldots, v_q, u_k, v_{q+1}, \ldots, v_{q+r}, v, v_{q+r+1}, \ldots, v_{q+r+s}\},$$
$$\lambda^2 = \{w_1, \ldots, w_n, v, w_{n+1}, \ldots, w_{n+m}, u_{k+1}, w_{n+m+1}, \ldots, w_{n+m+p}\}.$$

One can verify that $\{v_{q+1}, \ldots, v_{q+r}, v, w_{n+1}, \ldots, w_{n+m}\}$ is a cycle in $\mathcal{G}$ since the start node of v_{q+1} is the end node of w_{n+m}. This is in fact the end node of u_k, which is also the start node of u_{k+1} since λ is a path. This contradicts $\mathcal{G}$ being acyclic.

Thus, $\lambda = C$, and $\Lambda \subseteq \mathcal{C}$. In conclusion, $\mathcal{C} = \Lambda$.

□

Proof of Proposition 13. Let f^* and (ρ^*, μ^*) be optimal solutions of $(\mathcal{M}_P)$ and $(\mathcal{M}_D)$, respectively. From Lemma 13, we know that $(\mathcal{E}, \preceq_{\mathcal{G}})$ is a poset, whose set of maximal chains is the set of $s-t$ paths Λ. Thus, showing that there exists $\widetilde{\sigma}^2 \in \Delta(\mathcal{I})$ that satisfies (3.18) and (3.19) is an instantiation of problem $(\mathcal{D})$. Since (ρ^*, μ^*) is a feasible solution of $(\mathcal{M}_D)$, then condition (3.2) is satisfied, i.e., $\forall \lambda \in \Lambda,\ \sum_{(i,j)\in\lambda} \rho^*_{ij} \geq \pi^*_\lambda$. Additionally, for any $s-t$ path $\lambda \in \Lambda,\ \pi^*_\lambda = 1 - \sum_{(i,j)\in\lambda}(\frac{b_{ij}}{p_1} + \mu^*_{ij})$, and π^* is an affine function of the elements constituting each $s-t$ path. Therefore, π^* satisfies the conservation law described in (3.3). Finally, since $\forall (i,j) \in \mathcal{E},\ \rho^*_{ij} \in [0,1]$, and $\forall \lambda \in \Lambda,\ \pi^*_\lambda \leq 1$, all conditions of Theorem 4 are satisfied, and we obtain the existence of an interdiction strategy $\widetilde{\sigma}^2 \in \Delta(\mathcal{I})$ satisfying (3.18) and (3.19).

Next, we show that $(f^*, \widetilde{\sigma}^2)$ is a NE. We can write the following inequality for **P1**'s payoff:

$$\begin{aligned}
\forall f \in \mathcal{F},\ U_1(f, \widetilde{\sigma}^2) &\overset{(3.11)}{=} p_1 \sum_{\lambda\in\Lambda} f_\lambda \mathbb{E}_{\widetilde{\sigma}^2}[1 - \mathbb{1}_{\{I\cap\lambda\neq\emptyset\}}] - \sum_{\lambda\in\Lambda} b_\lambda f_\lambda \\
&= p_1 \sum_{\lambda\in\Lambda} \pi^0_\lambda f_\lambda - p_1 \sum_{\lambda\in\Lambda} f_\lambda \sum_{\{I\in\mathcal{I}\,|\,I\cap\lambda\neq\emptyset\}} \widetilde{\sigma}^2_I \\
&\overset{(3.19)}{\leq} p_1 \sum_{\lambda\in\Lambda} f_\lambda \sum_{(i,j)\in\lambda} \mu^*_{ij} = p_1 \sum_{(i,j)\in\mathcal{E}} f_{ij}\mu^*_{ij} \leq p_1 \sum_{(i,j)\in\mathcal{E}} c_{ij}\mu^*_{ij}. \quad (3.27)
\end{aligned}$$

Now, given $\lambda \in \Lambda$ such that $f^*_\lambda > 0$, we obtain:

$$\begin{aligned}
\sum_{\{I\in\mathcal{I}\,|\,I\cap\lambda\neq\emptyset\}} \widetilde{\sigma}^2_I \leq \sum_{I\in\mathcal{I}} \widetilde{\sigma}^2_I |I\cap\lambda| = \sum_{(i,j)\in\lambda} \sum_{I\in\mathcal{I}} \widetilde{\sigma}^2_I \mathbb{1}_{\{(i,j)\in I\}} &\overset{(3.18)}{=} \sum_{(i,j)\in\lambda} \rho^*_{ij} \\
&\overset{(3.17),(3.19)}{\leq} \sum_{\{I\in\mathcal{I}\,|\,I\cap\lambda\neq\emptyset\}} \widetilde{\sigma}^2_I. \quad (3.28)
\end{aligned}$$

Furthermore, $\forall (i,j) \in \mathcal{E}$ such that $\mu^*_{ij} > 0$, $f^*_{ij} \overset{(3.16)}{=} c_{ij}$. Then, inequality (3.27) is tight for f^*, and $U_1(f^*, \widetilde{\sigma}^2) = p_1 \sum_{(i,j)\in\mathcal{E}} c_{ij}\mu^*_{ij}$.

Similarly, regarding **P2**'s payoff, we first derive the following inequality:

$$\begin{aligned}\forall I \in \mathcal{I},\ \sum_{(i,j)\in I} \frac{d_{ij}}{p_2} &\geq \sum_{(i,j)\in I} \sum_{\{\lambda\in\Lambda \,|\, (i,j)\in\lambda\}} f^*_\lambda = \sum_{\lambda\in\Lambda} f^*_\lambda |I \cap \lambda| \\ &\geq \sum_{\lambda\in\Lambda} f^*_\lambda \mathbb{1}_{\{I\cap\lambda\neq\emptyset\}} = \mathrm{F}\left(f^*\right) - \mathrm{F}\left(f^{*I}\right). \end{aligned} \tag{3.29}$$

Therefore, $\forall I \in \mathcal{I},\ U_2(f^*, I) \overset{(3.12)}{=} p_2(\mathrm{F}\left(f^*\right) - \mathrm{F}\left(f^{*I}\right)) - \sum_{(i,j)\in I} d_{ij} \overset{(3.29)}{\leq} 0$.

Now, given $\lambda \in \Lambda$ such that $f^*_\lambda > 0$, we obtain:

$$\begin{aligned}\pi^0_\lambda - \sum_{(i,j)\in\lambda} \mu^*_{ij} &\overset{(3.17)}{=} \sum_{(i,j)\in\lambda} \rho^*_{ij} \overset{(3.18)}{=} \sum_{I\in\mathcal{I}} \widetilde{\sigma}^2_I |S \cap \lambda| \\ &\geq \sum_{\{I\in\mathcal{I} \,|\, I\cap\lambda\neq\emptyset\}} \widetilde{\sigma}^2_I \overset{(3.19)}{\geq} \pi^0_\lambda - \sum_{(i,j)\in\lambda} \mu^*_{ij}. \end{aligned} \tag{3.30}$$

Therefore, $\forall I \in \mathrm{supp}(\widetilde{\sigma}^2),\ |I \cap \lambda| \leq 1$. Furthermore, given $I \in \mathrm{supp}(\widetilde{\sigma}^2)$ and $(i,j) \in I$, $\sum_{\{\lambda\in\Lambda \,|\, (i,j)\in\lambda\}} f^*_\lambda \overset{(3.15)}{=} \frac{d_{ij}}{p_2}$, since $\rho^*_{ij} > 0$. Thus, $\forall I \in \mathrm{supp}(\widetilde{\sigma}^2)$, inequality (3.29) is tight, and $U_2(f^*, I) = 0$. Therefore, $U_2(f^*, \widetilde{\sigma}^2) = 0$, and $(f^*, \widetilde{\sigma}^2)$ is a NE. □

Proof of Theorem 6. Let $f^\dagger$ and $(\rho^\dagger, \mu^\dagger)$ be optimal solutions of $(\mathcal{M}_P)$ and $(\mathcal{M}_D)$ that satisfy strict complementary slackness. We denote $\widetilde{\sigma}^2 \in \Delta(\mathcal{I})$ the interdiction strategy, constructed from Algorithm 1, which interdicts every edge $(i,j) \in \mathcal{E}$ with probability $\rho^\dagger_{ij}$, and interdicts every $s-t$ path $\lambda \in \Lambda$ with probability at least $\pi^\dagger_\lambda \coloneqq \pi^0_\lambda - \sum_{(i,j)\in\lambda} \mu^\dagger_{ij}$. Given Σ the set of NE of the game Γ, let:

$$\begin{aligned}\mathcal{H}_1 &\coloneqq \bigcup_{(\sigma^{1*},\sigma^{2*})\in\Sigma} \bigcup_{f\in\mathrm{supp}(\sigma^{1*})} \{\lambda \in \Lambda \mid f_\lambda > 0\}, \\ \mathcal{H}_2 &\coloneqq \bigcup_{(\sigma^{1*},\sigma^{2*})\in\Sigma} \bigcup_{I\in\mathrm{supp}(\sigma^{2*})} I. \end{aligned}$$

From Proposition 13, we know that $(f^\dagger, \widetilde{\sigma}^2)$ is a NE. Consequently, $\mathcal{H}_1 \supseteq \mathrm{supp}(f^\dagger)$,

and $\mathcal{H}_2 \supseteq \text{supp}(\rho^\dagger)$. To show the reversed inclusions, we exploit properties of zero-sum games: Recall that the game Γ is strategically equivalent to the game $\widetilde{\Gamma} = \langle\{1,2\}, (\mathcal{F},\mathcal{I}), (\widetilde{u}_1, -\widetilde{u}_1)\rangle$ where $\widetilde{u}_1$ is given by (3.13). Therefore, each player's payoff in $\widetilde{\Gamma}$ is identical in any NE. We note the following equality:

$$\begin{aligned}\mathbb{E}_{\widetilde{\sigma}^2}[\mathrm{F}\left(f^\dagger\right) - \mathrm{F}\left(f^{\dagger I}\right)] &\overset{(3.30)}{=} \sum_{\lambda\in\Lambda} f^\dagger_\lambda \mathbb{E}_{\widetilde{\sigma}^2}[|I\cap\lambda|] \overset{(3.18)}{=} \sum_{\lambda\in\Lambda} f^\dagger_\lambda \sum_{(i,j)\in\lambda} \rho^\dagger_{ij} \\ &\overset{(3.21),(3.22)}{=} z^*_{(\mathcal{M})} - \sum_{(i,j)\in\mathcal{E}} c_{ij}\mu^\dagger_{ij}, \end{aligned} \tag{3.31}$$

where $z^*_{(\mathcal{M})}$ is the optimal value of $(\mathcal{M})$. This enables us to obtain **P1**'s equilibrium payoff in the zero-sum game $\widetilde{\Gamma}$: For every $(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma$,

$$\begin{aligned}\widetilde{U}_1(\sigma^{1^*},\sigma^{2^*}) &= \widetilde{U}_1(f^\dagger, \widetilde{\sigma}^2) \\ &\overset{(3.13)}{=} \mathbb{E}_{\widetilde{\sigma}^2}[\mathrm{F}\left(f^{\dagger I}\right)] - \mathrm{F}\left(f^\dagger\right) + \mathrm{F}\left(f^\dagger\right) - \frac{1}{p_1}\mathrm{T}(f^\dagger) + \frac{1}{p_2}\sum_{I\in\mathcal{I}} \widetilde{\sigma}^2_I \sum_{(i,j)\in I} d_{ij} \\ &\overset{(3.18)}{=} -\mathbb{E}_{\widetilde{\sigma}^2}[\mathrm{F}\left(f^\dagger\right) - \mathrm{F}\left(f^{\dagger I}\right)] + z^*_{(\mathcal{M})} + \frac{1}{p_2}\sum_{(i,j)\in\mathcal{E}} d_{ij}\rho^\dagger_{ij} \overset{(3.31)}{=} z^*_{(\mathcal{M})}. \end{aligned} \tag{3.32}$$

Consider $(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma$. Then, $(f^\dagger, \sigma^{2^*}) \in \Sigma$ as well. Thus:

$$\begin{aligned}\forall I \in \text{supp}(\sigma^{2^*}),\ z^*_{(\mathcal{M})} &\overset{(3.32)}{=} \widetilde{U}_1(f^\dagger, I) \\ &\overset{(3.13)}{=} \frac{1}{p_2}\mathrm{C}\left(I\right) + \mathrm{F}\left(f^{\dagger I}\right) - \mathrm{F}\left(f^\dagger\right) + \mathrm{F}\left(f^\dagger\right) - \frac{1}{p_1}\mathrm{T}(f^\dagger) \\ &\overset{(3.29)}{\geq} z^*_{(\mathcal{M})}. \end{aligned}$$

Therefore, for $I \in \text{supp}(\sigma^{2^*})$, (3.29) is tight, i.e., $\forall (i,j) \in I$, $\frac{d_{ij}}{p_2} = \sum_{\{\lambda\in\Lambda\,|\,(i,j)\in\lambda\}} f^\dagger_\lambda$. From (3.20), we deduce that $\forall (i,j) \in I$, $\rho^\dagger_{ij} > 0$, i.e., $(i,j) \in \text{supp}(\rho^\dagger)$. We can then conclude that $\mathcal{H}_2 \subseteq \text{supp}(\rho^\dagger)$, and we obtain that $\mathcal{H}_2 = \text{supp}(\rho^\dagger)$.

We now show the remaining inclusion for $\mathcal{H}_1$. Given $(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma$, we know that $(\sigma^{1^*}, \widetilde{\sigma}^2) \in \Sigma$ as well. Recall that $\forall S \in \text{supp}(\widetilde{\sigma}^2)$, (3.29) is tight. This implies that

for every $f \in \text{supp}(\sigma^{1^*})$,

$$z^*_{(\mathcal{M})} \overset{(3.32)}{=} \widetilde{U}_1(f, \widetilde{\sigma}^2) \overset{(3.13)}{=} \frac{1}{p_1} U_1(f, \widetilde{\sigma}^2) + \frac{1}{p_2} \mathbb{E}_{\widetilde{\sigma}^2}[\mathrm{C}\,(I)]$$
$$\overset{(3.29),(3.31)}{=} \frac{1}{p_1} U_1(f, \widetilde{\sigma}^2) + z^*_{(\mathcal{M})} - \sum_{(i,j)\in\mathcal{E}} c_{ij}\mu^\dagger_{ij} \overset{(3.27)}{\leq} z^*_{(\mathcal{M})}.$$

Therefore, $\forall f \in \text{supp}(\sigma^{1^*})$, (3.27) is tight, i.e.:

$$\forall \lambda \in \Lambda \mid f_\lambda > 0, \sum_{\{I\in\mathcal{I} \mid I\cap\lambda\neq\emptyset\}} \widetilde{\sigma}^2_I = \pi^0_\lambda - \sum_{(i,j)\in\lambda} \mu^\dagger_{ij}.$$

However, this is not enough to invoke strict complementary slackness (3.22). We also need to show (by contradiction) that $\forall I \in \text{supp}(\widetilde{\sigma}^2),\ \forall f \in \text{supp}(\sigma^{1^*}),\ \forall \lambda \in \Lambda$ such that $f_\lambda > 0$, we have $|I \cap \lambda| \leq 1$.

Let us assume that $\exists\,(I', f', \lambda') \in \text{supp}(\widetilde{\sigma}^2) \times \text{supp}(\sigma^{1^*}) \times \Lambda$ such that $f'_{\lambda'} > 0$ and $|I' \cap \lambda'| \geq 2$. Since I' interdicts at least two edges belonging to λ', which is taken by a flow in the support of σ^{1^*}, then we can construct another interdiction strategy $\sigma^{2'}$ that provides **P2** with a better payoff than $\widetilde{\sigma}^2$ does. This is done by reassigning some probability initially assigned to I' by $\widetilde{\sigma}^2$ to a non trivial partition of I'. This is possible because no interdiction $\emptyset$ belongs to the support of $\widetilde{\sigma}^2$, which is guaranteed by Theorem 5.

Specifically, from Theorem 5, we know that:

$$\widetilde{\sigma}^2_\emptyset = 1 - \max\{\max\{\rho^\dagger_{ij},\ (i,j) \in \mathcal{E}\}, \max\{\pi^\dagger_\lambda,\ \lambda \in \Lambda\}\}.$$

Since $\forall (i,j) \in \mathcal{E},\ b_{ij} > 0$ and $\mu^\dagger_{ij} \geq 0$, then $\forall \lambda \in \Lambda,\ \pi^\dagger_\lambda = 1 - \sum_{(i,j)\in\lambda}(\frac{b_{ij}}{p_1} + \mu^\dagger_{ij}) < 1$. By optimality of $\rho^\dagger$ in $(\mathcal{M}_D)$, we deduce that $\forall (i,j) \in \mathcal{E},\ \rho^\dagger_{ij} < 1$. Therefore, $\widetilde{\sigma}^2_\emptyset > 0$. Now, let $\epsilon = \min\{\widetilde{\sigma}^2_\emptyset, \widetilde{\sigma}^2_{I'}\} > 0$, and let $e \in I' \cap \lambda'$. Then, we construct the strategy $\sigma^{2'} \in \Delta(\mathcal{I})$ defined by $\sigma^{2'}_{I'} = \widetilde{\sigma}^2_{I'} - \epsilon$, $\sigma^{2'}_{I'\setminus\{e\}} = \widetilde{\sigma}^2_{I'\setminus\{e\}} + \epsilon$, $\sigma^{2'}_{\{e\}} = \widetilde{\sigma}^2_{\{e\}} + \epsilon$, $\sigma^{2'}_\emptyset = \widetilde{\sigma}^2_\emptyset - \epsilon$, and $\sigma^{2'}_I = \widetilde{\sigma}^2_I,\ \forall I \in \text{supp}(\widetilde{\sigma}^2)\setminus\{I', I'\setminus\{e\}, \{e\}, \emptyset\}$.

First, we note that the edge interdiction probabilities are preserved between $\widetilde{\sigma}^2$ and $\sigma^{2'}$, i.e., $\forall (i,j) \in \mathcal{E},\ \mathbb{E}_{\sigma^{2'}}[\mathbb{1}_{\{(i,j)\in I\}}] = \mathbb{E}_{\widetilde{\sigma}^2}[\mathbb{1}_{\{(i,j)\in I\}}] \overset{(3.18)}{=} \rho^\dagger_{ij}$. Secondly, each $s-t$

path $\lambda \in \Lambda$ is interdicted by $\sigma^{2'}$ with a probability no less than the probability with which λ is interdicted by $\widetilde{\sigma}^2$, i.e., $\forall \lambda \in \Lambda,\ \mathbb{E}_{\sigma^{2'}}[\mathbb{1}_{\{I\cap\lambda\neq\emptyset\}}] \geq \mathbb{E}_{\widetilde{\sigma}^2}[\mathbb{1}_{\{I\cap\lambda\neq\emptyset\}}]$. Thirdly, given λ', since $|I' \cap \lambda'| \geq 2$ and $e \in I' \cap \lambda'$, then $I'\backslash\{e\} \cap \lambda \neq \emptyset$ as well. This implies that $\mathbb{E}_{\sigma^{2'}}[\mathbb{1}_{\{I\cap\lambda'\neq\emptyset\}}] = \mathbb{E}_{\widetilde{\sigma}^2}[\mathbb{1}_{\{I\cap\lambda'\neq\emptyset\}}] + \epsilon$.

Putting everything together, we obtain:

$$U_2(\sigma^{1^*},\sigma^{2'}) \overset{(2.3)}{\geq} U_2(\sigma^{1^*},\widetilde{\sigma}^2) + p_2\mathbb{E}_{\sigma^{1^*}}[f_{\lambda'}\epsilon] \geq U_2(\sigma^{1^*},\widetilde{\sigma}^2) + p_2\sigma^{1^*}_{f'}f'_{\lambda'}\epsilon > U_2(\sigma^{1^*},\widetilde{\sigma}^2).$$

This contradicts $(\sigma^{1^*},\widetilde{\sigma}^2)$ being a NE. Therefore, we deduce that:

$$\forall I \in \text{supp}(\widetilde{\sigma}^2),\ \forall f \in \text{supp}(\sigma^{1^*}),\ \forall \lambda \in \Lambda \mid f_\lambda > 0,\ |I \cap \lambda| \leq 1.$$

Then, we obtain:

$$\forall f \in \text{supp}(\sigma^{1^*}),\ \forall \lambda \in \Lambda \mid f_\lambda > 0,\ \pi^0_\lambda - \sum_{(i,j)\in\lambda} \mu^\dagger_{ij} = \sum_{I\in\mathcal{I}} \widetilde{\sigma}^2_I \mathbb{1}_{\{I\cap\lambda\neq\emptyset\}} = \sum_{I\in\mathcal{I}} \widetilde{\sigma}^2_I |I\cap\lambda| \overset{(3.18)}{=} \sum_{(i,j)\in\lambda} \rho^\dagger_{ij}.$$

From (3.22), we deduce that $\forall f \in \text{supp}(\sigma^{1^*}),\ \forall \lambda \in \Lambda$ such that $f_\lambda > 0$, we have $f^\dagger_\lambda > 0$ as well, i.e., $\lambda \in \text{supp}(f^\dagger)$. Therefore, $\mathcal{H}_1 \subseteq \text{supp}(f^\dagger)$, and we can conclude that $\mathcal{H}_1 = \text{supp}(f^\dagger)$. □

Proof of Proposition 14. In (3.32), we established that $\forall(\sigma^{1^*},\sigma^{2^*}) \in \Sigma, \widetilde{U}_1(\sigma^{1^*},\sigma^{2^*}) = z^*_{(\mathcal{M})}$. Let f^* and (ρ^*,μ^*) denote optimal solutions of $(\mathcal{M}_P)$ and $(\mathcal{M}_D)$, respectively. Since $\forall(i,j) \in \mathcal{E},\ \frac{d_{ij}}{p_2} < c_{ij}$, then $\forall(i,j) \in \mathcal{E},\ f^*_{ij} \leq \frac{d_{ij}}{p_2} < c_{ij}$. Therefore, from (3.16), we deduce that $\forall(i,j) \in \mathcal{E},\ \mu^*_{ij} = 0$. Let $\widetilde{\sigma}^2 \in \Delta(\mathcal{I})$ denote the interdiction strategy constructed from Algorithm 1 that satisfies (3.18) and (3.19). We denote $f^0 \in \mathcal{F}$ the action of not sending any flow in the network, i.e., $f^0_\lambda = 0,\ \forall \lambda \in \Lambda$, and we denote $f' \coloneqq (1+\epsilon)f^*$, with $\epsilon = \min\{p_2\frac{c_{ij}}{d_{ij}} - 1,\ (i,j) \in \mathcal{E}\} > 0$. Then, $f' \in \mathcal{F}$.

Let us consider $\widetilde{\sigma}^1 \in \Delta(\mathcal{F})$ defined by: $\widetilde{\sigma}^1_{f'} = \frac{1}{1+\epsilon}$, and $\widetilde{\sigma}^1_{f^0} = \frac{\epsilon}{1+\epsilon}$. Then, we show that $(\widetilde{\sigma}^1,\widetilde{\sigma}^2)$ is a NE. Regarding **P1**'s payoff, since $\mu^*_{ij} = 0,\ \forall(i,j) \in \mathcal{E}$, we can rewrite

(3.27) as follows:

$$\forall f \in \mathcal{F},\ U_1(f, \widetilde{\sigma}^2) \overset{(3.11)}{=} p_1 \sum_{\lambda \in \Lambda} \pi^0_\lambda f_\lambda - p_1 \sum_{\lambda \in \Lambda} f_\lambda \sum_{\{I \in \mathcal{I} \,|\, I \cap \lambda \neq \emptyset\}} \widetilde{\sigma}^2_I$$
$$\overset{(3.19)}{\leq} p_1 \sum_{\lambda \in \Lambda} \pi^0_\lambda f_\lambda - p_1 \sum_{\lambda \in \Lambda} f_\lambda \pi^0_\lambda = 0.$$

Trivially, we obtain that $U_1(f^0, \widetilde{\sigma}^2) = 0$. Furthermore, we know from (3.28) that $\forall \lambda \in \Lambda$ such that $f^*_\lambda > 0,\ \sum_{\{I \in \mathcal{I} \,|\, I \cap \lambda \neq \emptyset\}} \widetilde{\sigma}^2_I = \pi^0_\lambda$. Since $f^*_\lambda > 0 \iff f'_\lambda > 0$, we deduce that $U_1(f', \widetilde{\sigma}^2) = 0$. Therefore $U_1(\widetilde{\sigma}^1, \widetilde{\sigma}^2) = 0$.

Regarding **P2**'s payoff, we know that $\forall \sigma^2 \in \Delta(\mathcal{I}),\ U_2(\widetilde{\sigma}^1, \sigma^2) = U_2(\mathbb{E}_{\widetilde{\sigma}^1}[f], \sigma^2) = U_2(f^*, \sigma^2)$. Therefore:

$$U_2(\widetilde{\sigma}^1, \widetilde{\sigma}^2) = U_2(f^*, \widetilde{\sigma}^2) \geq U_2(f^*, \sigma^2) = U_2(\widetilde{\sigma}^1, \sigma^2),\ \forall \sigma^2 \in \Delta(\mathcal{I}).$$

Thus, $(\widetilde{\sigma}^1, \widetilde{\sigma}^2)$ is a NE.

We now consider $(\sigma^{1^*}, \sigma^{2^*}) \in \Sigma$. Then, we know that $(\sigma^{1^*}, \widetilde{\sigma}^2) \in \Sigma$ and $(\widetilde{\sigma}^1, \sigma^{2^*}) \in \Sigma$. Since $f^0 \in \text{supp}(\widetilde{\sigma}^1)$, we obtain that $p_2 \widetilde{U}_1(f^0, \sigma^{2^*}) \overset{(3.13)}{=} \mathbb{E}_{\sigma^{2^*}}[\mathrm{C}(I)] \overset{(3.32)}{=} p_2 z^*_{(\mathcal{M})}$. Similarly, since $\emptyset \in \text{supp}(\widetilde{\sigma}^2)$, then $p_1 \widetilde{U}_1(\sigma^{1^*}, \emptyset) \overset{(3.13)}{=} \mathbb{E}_{\sigma^{1^*}}[p_1 \mathrm{F}(f) - \mathrm{T}(f)] \overset{(3.32)}{=} p_1 z^*_{(\mathcal{M})}$. We deduce the players' equilibrium payoffs:

$$U_1(\sigma^{1^*}, \sigma^{2^*}) \overset{(3.13)}{=} p_1 \widetilde{U}_1(\sigma^{1^*}, \sigma^{2^*}) - \frac{p_1}{p_2} \mathbb{E}_{\sigma^{2^*}}[\mathrm{C}(I)] \overset{(3.32)}{=} p_1 z^*_{(\mathcal{M})} - p_1 z^*_{(\mathcal{M})} = 0,$$
$$U_2(\sigma^{1^*}, \sigma^{2^*}) \overset{(3.14)}{=} p_2(-\widetilde{U}_1(\sigma^{1^*}, \sigma^{2^*})) + p_2 \mathbb{E}_{\sigma^{2^*}}[\mathrm{F}(f) - \frac{1}{p_1} \mathrm{T}(f)] \overset{(3.32)}{=} 0.$$

Finally, we characterize the expected amount of flow that is interdicted in any equilibrium: $\mathbb{E}_{\sigma^*}[\mathrm{F}(f) - \mathrm{F}\left(f^I\right)] = \frac{1}{p_2} U_2(\sigma^{1^*}, \sigma^{2^*}) + \frac{1}{p_2} \mathbb{E}_{\sigma^{2^*}}[\mathrm{C}(I)] = z^*_{(\mathcal{M})}$. □

Proof of Lemma 14. Let (ρ^*, μ^*) be an optimal solution of $(\mathcal{M}_D)$, and let $(e_1, e_2) \in \text{supp}(\rho^*)^2$. We denote r the root of the minimal subtree of $\mathcal{T}_\mathcal{G}$ that contains e_1 and e_2. Let $\mathcal{G}_1$ (resp. $\mathcal{G}_2$) denote the graph represented by the child of r that contains e_1 (resp. e_2)

– If $r = P_c$ (i.e., e_1 and e_2 are in parallel), then we can show by contradiction that

there is no path in $\mathcal{G}$ that goes through e_1 and e_2. Indeed, if there were one, it would create a Wheatstone bridge and would contradict $\mathcal{G}$ being an SP-graph; see Figure 3-16.

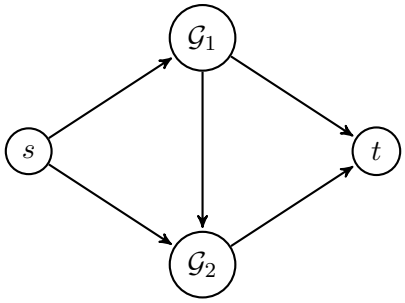


Figure 3-16: Proof that if two subgraphs of an SP-graph are in parallel, then there is no path that goes through both of them.

– If $r = S_c$ (i.e., e_1 and e_2 are in series), then we know by definition that $t_{\mathcal{G}_1} = s_{\mathcal{G}_2}$. Now, consider an optimal solution f^* of $(\mathcal{M}_P)$. From complementary slackness (3.15), we deduce that $f^*_{e_1} = \frac{d_{e_1}}{p_2} > 0$. Similarly, $f^*_{e_2} > 0$. Therefore, $\exists\,(\lambda_1, \lambda_2) \in \Lambda^2 \mid f^*_{\lambda_1} > 0,\ f^*_{\lambda_2} > 0,\ e_1 \in \lambda_1$ and $e_2 \in \lambda_2$.

If $e_2 \in \lambda_1$ or $e_1 \in \lambda_2$, then we get the expected result. On the other hand, if $e_2 \notin \lambda_1$ and $e_1 \notin \lambda_2$, then we can note that both paths λ_1 and λ_2 go through the same node $t_{\mathcal{G}_1} = s_{\mathcal{G}_2}$; see Figure 3-17.

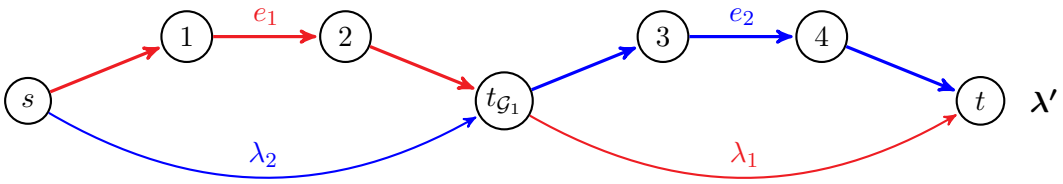


Figure 3-17: Proof that if two edges in the support of ρ^* are in series in an SP-graph, then there is a path (in thick line) taken by an optimal flow that goes through both of them.

We can then partition λ_1 into λ_1^{start} and λ_1^{end}, depending on the edges in λ_1 that are before or after $t_{\mathcal{G}_1}$. Similarly, we partition λ_2 into $\lambda_2^{start} \cup \lambda_2^{end}$. Then we can construct another optimal flow f' by removing ϵ units of flow from f^* along

the paths λ_1 and λ_2, and adding ϵ units of flow through $\lambda' = \lambda_1^{start} \cup \lambda_2^{end}$ and $\lambda_2^{start} \cup \lambda_1^{end}$. Note that $e_1 \in \lambda'$, $e_2 \in \lambda'$, and $f'_{\lambda'} > 0$, which proves the result.

□

Chapter 4

Analytics-Driven Inspection for Localizing Post-Disaster Failures

4.1 Introduction

In this chapter, we consider the problem of optimal scheduling of inspection operations for a utility company that has access to imperfect diagnostic information (e.g., sensor alerts, customer calls, incident reports) regarding the failure locations in different parts of its distribution network after a major natural disaster. The goal is to determine an inspection strategy, i.e., the scheduling of sites to inspect, to maximize the expected reward obtained from successfully identifying failure locations in the network, while also ensuring that the time constraints faced by inspection teams are satisfied.

We model this problem as a stochastic team orienteering problem in which a set of sites needs to be inspected by inspection teams for likely failures. We then identify the key features of the optimal solution and use them to provide both exact and approximate solution approaches to the problem. The resulting strategies prescribe deterministic inspection schedules, and capture the essential tradeoff between the travel time between sites, the inspection time of each site, the imperfect diagnostic information, and the available inspection time.

More broadly, our work addresses the need to integrate predictive models of fail-

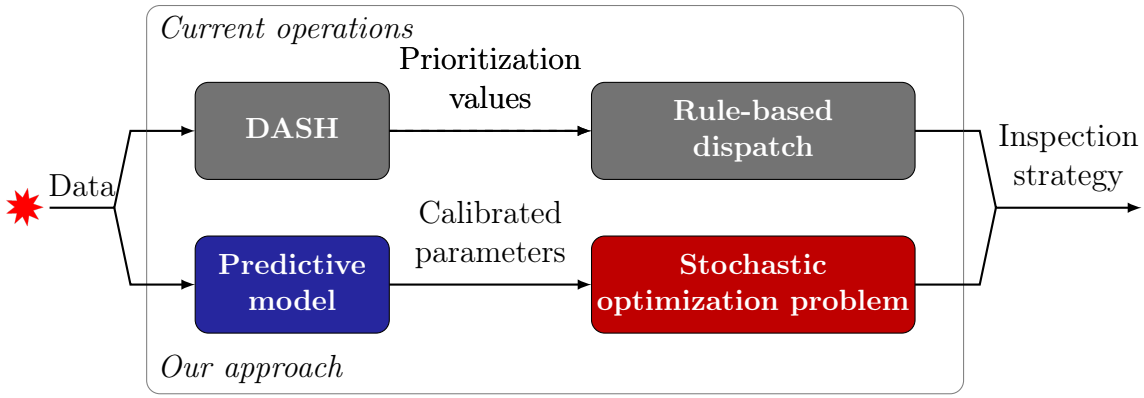


Figure 4-1: Scheduling of response operations.

ures into the emergency response and repair operations of infrastructure utilities [6]. Currently, utilities conduct inspection operations either based on a set of a priori fixed schedules, or on an as-needed basis after receiving customer calls. On one hand, the downside of fixed schedules is that they are not able to address critical disruptions in a timely manner, and can contribute to increased non-revenue losses for the utilities. On the other hand, experiential evidence suggests that the as-needed response strategies may be prone to gaming by customers who misreport or misjudge failure alerts. Thus, inspection strategies that account for the value of addressing these failures (i.e., criticality) as well as the likelihood of finding failure events in different sites are desirable. Fortunately, in recent years, utilities have been spending significant efforts in collecting the data relevant for estimating the failure probabilities and the value of service restoration for various sites. This data can be used to calibrate the stochastic orienteering model defined in this work. In particular, the probability of finding failures within each site can be estimated by building a statistical model using the data on properties of distribution pipelines, geological data (e.g., ground motion prediction equations), and the output of damage modeling software. The site-specific values of service restoration are also obtained using data on inspection costs and revenue losses. See Figure 4-1 for a summary of contributions.

Note that this inspection problem is related to previous work on stochastic knapsack [27], stochastic orienteering [45], and stochastic probing [46]. The main progress achieved by the above-mentioned literature is the design of approximation algorithms

which provide efficient nonadaptive strategies, with bounds on the optimality gaps relative to optimal adaptive solutions. Instead, we exploit the features of the problem to derive exact optimization-based approaches to compute optimal nonadaptive strategies. They rely on a linear recurrence relation satisfied by sites visited along a same route by an inspection team. We also investigate and compare approximate solution approaches based on greedy (myopic) procedures and deterministic optimization models.

We then design a computational study to evaluate and compare the various solution approaches by solving multiple instances of the problem. We find that on average, our greedy algorithm performs reasonably well, and that our formulation based on an extension of the truncated knapsack orienteering problem performs extremely well. However, we noted instances for which these approximate approaches provided solutions with optimality gaps reaching 80% and 60%, respectively. This shows the value of being able to optimally solve our stochastic team orienteering problem using our exact optimization-based approaches.

The rest of this chapter is organized as follows: In Section 4.2 we formulate our inspection problem as a stochastic optimization problem. Section 4.3 presents our exact and approximate solution methods. In Section 4.4, we evaluate and compare our solution methods using our computation study. Finally, we provide some concluding remarks in Section 4.5 and derive the proofs of our results in Section 4.6.

4.2 Problem Formulation

Consider the setting where a utility is concerned with dispatching its inspection teams to localize failures within its distribution network in the aftermath of a natural disaster. Specifically, after a natural disaster event occurs, component failures occur within the distribution network and need to be fixed. However, their locations are often unknown, and the utility dispatches inspection teams to survey parts of the network and determine whether or not they contain failures. Let $\mathcal{V}$ be the set of sites that potentially contain failures. Typically, when an inspection team surveys a site,

it checks the distribution network within that site with detectors. If a failure is identified by the team, it is reported to the utility, which then schedules the dispatch of repair teams. Once the inspection of a site is completed, the inspection team travels to another site for inspection.

After a natural disaster occurs, the utility gathers information regarding the state of its infrastructure. This information is generally gathered from different sources, such as fixed sensors placed within the distribution network or calls from customers and emergency services. In addition, the utility analyzes other type of data, such as information on the natural disaster itself, but also regarding the environment surrounding the distribution network. For instance, power lines that are surrounded by trees are most likely to go down after a hurricane. Another example for natural gas networks is that pipelines that are next to a fault line have a higher chance to be damaged during an earthquake. Using this data, the utility obtains diagnostic information regarding the state of its network [68].

We consider that for each site $i \in \mathcal{V}$, there are n_i possible failure scenarios. For instance, a scenario may represent the number of failures present in the site. If the utility has less information, a scenario may only represent whether a site contains no failures, a small number of failures, or a large number of failures. For each site $i \in \mathcal{V}$ and possible failure scenario $k \in [\![1, n_i]\!]$, we consider a criticality level v_i^k and a discrete random inspection time T_i^k. The criticality level is usually determined from the cost of damage associated with a failure scenario within a particular site. It can also account for the importance of a site. In practice, it is determined from the number of failures within the site, the number of people living in the site (if this is a residence), whether or not this is a school, hospital, etc. The inspection time T_i^k is assumed to be random for a given site i and failure scenario k because of the uncertainty in the distribution of failures within a site. For instance, there are settings where the inspection team will stop the inspection of a site as soon as it finds a failure. The reason is that when it is determined that a site contains at least one failure, a repair team will be scheduled to fix it. For security purposes, when repair teams come to a site, they also conduct a final inspection to clear the site. Therefore,

in this setting, the time to "complete" the inspection of a site depends on when the first failure is found, which is uncertain. Note that no further assumption is made on T_i^k. This allows us to consider different inspection times for different scenarios. This is a desirable feature when for instance the inspection time of a site depends on the number of failures. Note that when determining T_i^k, we can account for the characteristics of the network in site i, the sensing capabilities of the detectors, as well as prior knowledge regarding failure locations within site i (e.g., due to experience). Let f_i^k denote the probability mass function of T_i^k. Without loss of generality, we assume that the inspection time T_i^k is positive with positive probability.

We consider that the diagnostic information from analytics models [68] determines a probability distribution over failure scenarios for each site. Specifically, for each site $i \in \mathcal{V}$, we denote B_i the random variable that characterizes the failure scenario in i. For each failure scenario $k \in [\![1, n_i]\!]$, $\pi_i^k \coloneqq \mathbb{P}(B_i = k)$. Then, the marginal inspection time of site $i \in \mathcal{V}$, which we denote by T_i, with probability mass function f_i, is such that:

$$\forall s \geq 0,\ f_i(s) = \sum_{k=1}^{n_i} \pi_i^k f_i^k(s).$$

The utility has b inspection teams that can be simultaneously dispatched for localizing the failures. Without loss of generality, we consider that all teams leave from the same yard s_0. For each pair of locations $i \neq j \in \{s_0\} \cup \mathcal{V}$, we denote t_{ij} the symmetric travel time between i and j. In post-disaster settings, time is a crucial resource. In particular, the goal of response operations is to address failures in a timely manner. Thus, we consider a time budget T_{Total} during which inspection teams operate. T_{Total} typically represents a day of operations. Then, the utility is interested in scheduling the dispatch of its b inspection teams so that it maximizes the reward obtained from localizing failures within the time budget T_{Total}. In particular, the utility receives the reward v_i^k if an inspection team completes the inspection of site i under scenario k before time T_{Total}. For simplicity, we consider discrete units of time, and assume that each time quantity presented in this model can be expressed as a multiple of the time unit. Without loss of generality, we let the time unit be 1.

Thus, the Post-Disaster Inspection Problem (PDIP) is a team orienteering problem with stochastic rewards and service (i.e., inspection) times. For this problem, we focus on the study of nonadaptive strategies. Indeed, certain utilities do not currently have the means to incorporate new information within a day of operations, and cannot change the scheduling of their teams to adapt to the realization of uncertainty as the teams inspect new sites. Utilities instead determine fixed scheduling of their operations that they decide at the beginning of each day of operations. Then, each team inspects sites as dictated by their assigned schedule, and stop whenever they reach the end of their schedule or they reach the time limit T_{Total}.

The PDIP then consists of finding b routes originating at yard s_0 and that maximize:

$$\begin{aligned}
&\sum_{i\in\mathcal{V}} \mathbb{E}[\text{Reward from inspecting site } i] \\
=&\sum_{i\in\mathcal{V}}\sum_{k=1}^{n_i} \mathbb{E}[\text{Reward from inspecting site } i \mid B_i = k]\mathbb{P}(B_i = k) \\
=&\sum_{i\in\mathcal{V}}\sum_{k=1}^{n_i} v_i^k \pi_i^k \mathbb{P}(\text{Inspection of site } i \text{ is completed before } T_{Total} \mid B_i = k).
\end{aligned}$$

A route p originating at yard s_0 is represented by a sequence of nodes $\{i_0, \ldots, i_n\}$ with $i_0 = s_0$. Let $\mathcal{P}$ denote the set of routes originating at yard s_0. Then, given a route $p = \{i_0, \ldots, i_n\} \in \mathcal{P}$, the time to complete the inspection of the $l-$th site visited along that route under the failure scenario $k \in [\![1, n_{i_l}]\!]$ is given by the random variable $\sum_{j=1}^{l-1} T_{i_j} + T_{i_l}^k + \sum_{j=0}^{l-1} t_{i_j,i_{j+1}}$, which is composed of the (deterministic) travel time to reach site i_l, the (random) marginal inspection time of each site i_j, for $j \in [\![1, l-1]\!]$, and the (random) inspection time of site i_l under scenario k.

We suppose that the utility does not schedule different teams to inspect the same site within the same day of operations. Let $\mathcal{A}$ denote the set of possible schedules. $\mathcal{A}$ is defined as follows:

$$\mathcal{A} = \{(p_1, \ldots, p_b) \in \mathcal{P}^b \mid p_i \cap p_j = \{s_0\},\ \forall i \neq j \in [\![1, b]\!]\}.$$

For notational convenience, given a scheduling of operations $(p_1, \ldots, p_b) \in \mathcal{A}$, we denote $p_i = \{i_0, \ldots, i_{m_i}\}$, with m_i being the number of sites in route p_i. Then, the mathematical formulation of the PDIP is given using the following stochastic optimization problem:

$$\max_{(p_1,\ldots,p_b)\in\mathcal{A}} \sum_{i=1}^{b}\sum_{l=1}^{m_i}\sum_{k=1}^{n_{i_l}} v_{i_l}^k \pi_{i_l}^k \mathbb{P}(\text{Inspection of site } i_l \text{ is completed before } T_{Total} \mid B_{i_l} = k)$$

$$= \max_{(p_1,\ldots,p_b)\in\mathcal{A}} \sum_{i=1}^{b}\sum_{l=1}^{m_i}\sum_{k=1}^{n_{i_l}} v_{i_l}^k \pi_{i_l}^k \mathbb{P}\Big(\sum_{j=1}^{l-1} T_{i_j} + T_{i_l}^k \leq T_{Total} - \sum_{j=0}^{l-1} t_{i_j,i_{j+1}}\Big). \tag{4.1}$$

The PDIP is an NP-hard problem. It contains an exponential number of feasible solutions and the objective function itself requires an exponential number of operations to be evaluated. Indeed, given a scheduling of operations $(p_1, \ldots, p_b) \in \mathcal{A}$, the corresponding objective function is given by:

$$\sum_{i=1}^{b}\sum_{l=1}^{m_i}\sum_{k=1}^{n_{i_l}} v_{i_l}^k \pi_{i_l}^k \sum_{s_1=0}^{T_{total}} \cdots \sum_{s_l=0}^{T_{total}} \left(\prod_{j=1}^{l-1} f_{i_j}(s_j)\right) f_{i_l}^k(s_l) \mathbb{1}_{\{s_1+\cdots+s_l \leq T_{Total} - \sum_{j=0}^{l-1} t_{i_j,i_{j+1}}\}}. \tag{4.2}$$

Next, we show that (4.2) satisfies some properties that enable us to provide a solution approach to the PDIP.

4.3 Solution Approaches

In this section, we exploit the features of the model to propose two mixed-integer programming problems that optimally solve the PDIP. We then define three approximate solution approaches, based on a greedy algorithm, a certainty equivalent mixed-integer program, and an extension of the truncated knapsack orienteering problem.

4.3.1 Exact Methods

In Section 4.2 we formulated the PDIP as a stochastic optimization problem; see (4.1). However, the objective function requires an exponential number of operations to be evaluated. Thus, we derive properties satisfied by solutions of the PDIP that

we will leverage in our solution approaches.

Consider a route $p_i = \{i_0, \ldots, i_{m_i}\} \in \mathcal{P}$, and for each $l \in [\![0, m_i - 1]\!]$, let $z^*_{i_l}$ be defined as follows:

$$\forall l \in [\![0, m_i - 1]\!],\ \forall t \in \mathbb{Z},\ z^*_{i_l}(t) = \mathbb{P}(\sum_{j=1}^{l} T_{i_j} \leq t - \sum_{j=0}^{l-1} t_{i_j, i_{j+1}}). \tag{4.3}$$

The quantity $z^*_{i_l}(t)$ represents the probability that the inspection of the $l-$th site visited along route p_i is completed before time t.

Then, we can rewrite the PDIP as follows:

$$\begin{aligned}
&\max_{(p_1,\ldots,p_b)\in\mathcal{A}} \sum_{i=1}^{b}\sum_{l=1}^{m_i}\sum_{k=1}^{n_{i_l}} v^k_{i_l}\pi^k_{i_l} \sum_{s=0}^{T_{Total}} f^k_{i_l}(s)\mathbb{P}(\sum_{j=1}^{l-1} T_{i_j} \leq T_{Total} - s - t_{i_{l-1},i_l} - \sum_{j=0}^{l-2} t_{i_j,i_{j+1}}) \\
\overset{(4.3)}{=} &\max_{(p_1,\ldots,p_b)\in\mathcal{A}} \sum_{i=1}^{b}\sum_{l=1}^{m_i}\sum_{k=1}^{n_{i_l}} v^k_{i_l}\pi^k_{i_l} \sum_{s=0}^{T_{Total}-t_{i_{l-1},i_l}} f^k_{i_l}(s) z^*_{i_{l-1}}(T_{Total} - t_{i_{l-1},i_l} - s).
\end{aligned}$$

We show the following result:

Lemma 15. *Given a route $p_i = \{i_0, \ldots, i_{m_i}\} \in \mathcal{P}$, the quantity z^* defined in (4.3) satisfies the following properties:*

$$\forall t \in \mathbb{Z},\ z^*_{i_0}(t) = \mathbb{1}_{\{t\geq 0\}}, \tag{4.4}$$

$$\forall l \in [\![1, m_i - 1]\!],\ \forall t \in \mathbb{Z},\ z^*_{i_l}(t) = \sum_{s=0}^{t-t_{i_{l-1},i_l}} f_{i_l}(s) z^*_{i_{l-1}}(t - t_{i_{l-1},i_l} - s). \tag{4.5}$$

Thus, although $z^*_{i_l}(t)$ would have required $O(T^l_{Total})$ operations if computed using (4.2), it can now be computed using $O(l \times T_{Total})$ operations and $O(l \times T_{Total})$ memory. Most importantly, in Lemma 15, we obtained a linear recurrence relation satisfied by z^*. Next, we leverage this result to formulate a mixed-integer programming formulation of the PDIP. For each pair of locations $(i, j) \in (\{s_0\} \cup \mathcal{V})^2 \mid i \neq j$, we define the binary variable x_{ij} equal to 1 if an inspection team goes from i to j, and 0 otherwise. Then, for each pair of locations $i \neq j \in \{s_0\} \cup \mathcal{V}$, and each time $t \in [\![0, T_{Total}]\!]$, we define the continuous variable z^t_{ij}, which represents the probability with which the

inspection of site i is completed before time t, if a team travels from i to j. The PDIP can then be solved with the following mixed-integer program, which we denote (IP_1):

$$\max \quad \sum_{i\in\mathcal{V}} \sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} \sum_{s=0}^{T_{Total}-t_{ji}} \sum_{k=1}^{n_i} v_i^k \pi_i^k f_i^k(s) z_{ji}^{T_{Total}-t_{ji}-s} \tag{4.6}$$

$$\text{s.t.} \sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} x_{ji} \leq 1, \qquad \forall i \in \mathcal{V} \tag{4.7}$$

$$\sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} x_{ij} = \sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} x_{ji}, \qquad \forall i \in \mathcal{V} \tag{4.8}$$

$$\sum_{j\in\mathcal{V}} x_{s_0 j} = b, \tag{4.9}$$

$$z_{ij}^t \leq x_{ij}, \qquad \forall i \neq j \in \mathcal{V}\cup\{s_0\},\ \forall t \in [\![0, T_{Total}]\!] \tag{4.10}$$

$$\sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} z_{ij}^t \leq \sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} \sum_{s=0}^{t-t_{ji}} f_i(s) z_{ji}^{t-t_{ji}-s},\ \forall i \in \mathcal{V},\ \forall t \in [\![0, T_{Total}]\!] \tag{4.11}$$

$$x_{ij} \in \{0,1\}, \qquad \forall i \neq j \in \mathcal{V}\cup\{s_0\}$$

$$z_{ij}^t \geq 0, \qquad \forall i \neq j \in \mathcal{V}\cup\{s_0\},\ \forall t \in [\![0, T_{Total}]\!].$$

Constraints (4.7) ensure that each site is visited by at most one team. Constraints (4.8) ensure the continuity of each route taken by a team. In other words, if a team travels to site $i \in \mathcal{V}$, it must then leave it. Constraint (4.9) models the fact that b teams are dispatched from the yard s_0. Constraints (4.10) ensure that for every time $t \in [\![0, T_{Total}]\!]$, z_{ij}^t is nonzero only if a team travels from location $i \in \mathcal{V}\cup\{s_0\}$ to another location $j \in \mathcal{V}\cup\{s_0\}$. Most importantly, constraints (4.11) update the z values as a team travels along a route. Although constraints (4.11) are formulated with inequalities, they become tight at optimality. Formulating them as inequality constraints rather than equality constraints proved to significantly speed the solution of (IP_1). Objective (4.6) then represents the reward obtained by traveling along the routes defined by the x variables. Note that we do not require each site to be visited.

Typically, the total number of sites is significantly larger than the number of sites that can be inspected within a day of operations. We then have the following result:

Proposition 15. *(IP_1) is a mixed-integer programming formulation of the PDIP.*

Interestingly, this formulation does not require subtour elimination constraints. Indeed, although an optimal solution of (IP_1) may contain subtours, these subtours do not contribute to the objective function. The reason is that the only feasible value of the z variables that satisfies constraints (4.11) along a cycle that does not contain s_0 is 0. On the other hand, for a given route originating at s_0, constraints (4.11) will sequentially update the z values using the recurrence relation (4.4)-(4.5), which will ensure that at each site $i \in \mathcal{V}$, z_{ij}^t represents the probability with which the inspection of site i is completed before time t. Note that this is possible because each site can only be visited by at most one team per day of operations (constraints (4.7)).

One limitation of (IP_1) is that it contains $O(T_{Total}|\mathcal{V}|^2)$ variables and constraints. Thus, the size of (IP_1) can become too large for large-scale networks and a fine time discretization of the day of operations. Next, we propose another mixed-integer programming formulation of the PDIP that requires less variables. In this formulation, we again consider a binary variable x_{ij} for each pair of locations $(i, j) \in (\{s_0\} \cup \mathcal{V})^2 \mid i \neq j$ that determines whether or not a team travels from i to j. Then, for each location $i \in \mathcal{V} \cup \{s_0\}$, failure scenario $k \in [\![1, n_i]\!]$, and time $t \in [\![0, T_{Total}]\!]$, we define the real variable $z_{i,k}^t$, which represents the probability with which the inspection of site i under scenario k is completed before time t. The PDIP can then be solved with the

following mixed-integer program, which we denote (IP_2):

$$\max \quad \sum_{i\in\mathcal{V}}\sum_{k=1}^{n_i} v_i^k \pi_i^k z_{i,k}^{T_{Total}} \tag{4.12}$$

$$\text{s.t.} \quad \sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} x_{ji} = 1, \qquad \forall i \in \mathcal{V} \tag{4.13}$$

$$\sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} x_{ij} = 1, \qquad \forall i \in \mathcal{V} \tag{4.14}$$

$$\sum_{j\in\mathcal{V}} x_{s_0 j} = b, \tag{4.15}$$

$$z_{s_0,k}^t = 1, \qquad \forall k \in [\![1, n_{s_0}]\!], \forall t \in [\![0, T_{Total}]\!] \tag{4.16}$$

$$z_{i,k}^t \leq \sum_{s=0}^{t-t_{ji}} f_i^k(s) \sum_{k'=1}^{n_j} \pi_j^{k'} z_{j,k'}^{t-t_{ji}-s} + (1 - x_{ji}), \ \forall i \in \mathcal{V}, \forall j \in \mathcal{V}\cup\{s_0\}, \forall k \in [\![1, n_i]\!], \ \forall t \in [\![0, T_{Total}]\!] \tag{4.17}$$

$$x_{ij} \in \{0, 1\}, \qquad \forall i \neq j \in \mathcal{V}\cup\{s_0\}$$

$$z_{i,k}^t \geq 0, \qquad \forall i \in \mathcal{V}\cup\{s_0\}, \ \forall k \in [\![1, n_i]\!], \ \forall t \in [\![0, T_{Total}]\!].$$

Constraints (4.16) initialize the z variables at the yard. Then, constraints (4.17) ensure the linear recurrence between the z variables holds along each route. Specifically, if a team travels from j to i, then the right-hand side represents the probability with which the inspection of site i under scenario k is completed before time t, given that the team previously inspected site j. Note that if no team travels from j to i, then the right-hand side is at least 1 and does not constrain the z variables at location i. In contrast to (IP_1), constraints (4.13)-(4.14) require that each location be visited by a team. This ensures that at least one of the right-hand sides for constraints (4.17) has $x_{ji} = 1$ and bounds the z variables. As a result, the optimal solution will require that each location be visited by a team, even if the potential reward is 0 (because the probability of inspecting that site before T_{Total} is 0). Similarly to (IP_1), if an optimal solution contains a cycle, constraints (4.17) ensure that the z variables for each location within that cycle are all equal to 0 and do not contribute to the objective

function. We have the following result:

Proposition 16. *(IP_2) is a mixed-integer programming formulation of the PDIP.*

In contrast to (IP_1), (IP_2) requires $O(T_{Total} \sum_{i \in \mathcal{V}} n_i + |\mathcal{V}|^2)$ variables and $O(T_{Total}|\mathcal{V}| \sum_{i \in \mathcal{V}} n_i)$ constraints. Whenever the number of failure scenarios per site is small, the size of (IP_2) is significantly smaller than that of (IP_1). However, the linear programming relaxation of (IP_1) is tighter than that of (IP_2), which results in mixed-integer programming solvers being significantly slower at solving (IP_2) than at solving (IP_1), despite (IP_2)'s smaller size. Next, we present three solution approaches to approximately solve the PDIP.

4.3.2 Approximation Methods

We investigate three solution approaches that approximately solve the PDIP. First, we consider a greedy algorithm that sequentially and myopically assigns a site to each team. At each iteration, the algorithm selects a team, and appends its route (currently ending at site i) with the site j that maximizes the performance metric:

$$\frac{\sum_{k=1}^{n_j} v_j^k \pi_j^k}{t_{ij} + \sum_{s \geq 0} s f_j(s)}.$$

The premise is that teams should travel to sites that achieve a tradeoff between expected reward, travel time, and expected inspection time. This greedy algorithm is detailed in Algorithm 4.

The second approach is based on the certainty equivalent formulation of the PDIP. Specifically, we assign to each site $i \in \mathcal{V}$ the expected reward $\sum_{k=1}^{n_i} v_i^k \pi_i^k$ and the expected inspection time $\sum_{s \geq 0} s f_i(s)$. Then, we consider the deterministic optimization problem, which consists of selecting a scheduling of operations that maximizes the expected reward from the visited sites, while ensuring that the travel time plus the expected inspection time for each team does not exceed T_{Total}. The formulation is

Algorithm 4 : Greedy Algorithm

Input: Yard s_0, set of sites $\mathcal{V}$, number of inspection teams b, failure scenarios data (v_i^k, π_i^k, f_i^k), $\forall i \in \mathcal{V},\ \forall k \in [\![1, n_i]\!]$, travel times t_{ij}, $\forall i \neq j \in \{s_0\} \cup \mathcal{V}$.

Output: Scheduling of operations $(p_1, \ldots, p_b) \in \mathcal{A}$.

$\mathcal{L} \leftarrow \mathcal{V}$

$p_\ell \leftarrow [s_0]$, $\forall \ell \in [\![1, b]\!]$

$m \leftarrow 1$

while $\mathcal{L} \neq \emptyset$ **do**

    $i \leftarrow p_m[end]$

    $j^* \leftarrow \arg\max_{j \in \mathcal{L}} \dfrac{\sum_{k=1}^{n_j} v_j^k \pi_j^k}{t_{ij} + \sum_{s \geq 0} s f_j(s)}$.

    $p_m \leftarrow [p_m, j^*]$

    $\mathcal{L} \leftarrow \mathcal{L} \backslash \{j^*\}$

    if $m < b$ **then**

        $m \leftarrow m + 1$

    else if $m = b$ **then**

        $m \leftarrow 1$

    end if

end while

given as follows:

$$\max \quad \sum_{i\in\mathcal{V}}\sum_{k=1}^{n_i} v_i^k \pi_i^k \sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} x_{ji} \tag{4.18}$$

$$\text{s.t.} \sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} x_{ji} \leq 1, \qquad \forall i \in \mathcal{V} \tag{4.19}$$

$$\sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} x_{ij} = \sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} x_{ji}, \qquad \forall i \in \mathcal{V} \tag{4.20}$$

$$\sum_{j\in\mathcal{V}} x_{s_0 j} = b, \tag{4.21}$$

$$y_{s_0 j} = (t_{s_0 j} + \sum_{s\geq 0} s f_j(s)) x_{s_0 j}, \qquad \forall j \in \mathcal{V} \tag{4.22}$$

$$y_{ij} \leq T_{Total} x_{ij}, \qquad \forall (i,j) \in (\mathcal{V}\cup\{s_0\}) \times \mathcal{V} \mid i \neq j \tag{4.23}$$

$$\sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} y_{ij} = \sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} y_{ji} + \sum_{\substack{j\in\mathcal{V}\\ j\neq i}} (t_{ij} + \sum_{s\geq 0} s f_j(s)) x_{ij}, \quad \forall i \in \mathcal{V} \tag{4.24}$$

$$x_{ij} \in \{0,1\}, \qquad \forall i \neq j \in \mathcal{V}\cup\{s_0\}$$

$$y_{ij} \geq 0, \qquad \forall i \neq j \in \mathcal{V}\cup\{s_0\}.$$

Constraints (4.19)-(4.21) create b routes that will be taken by the teams. Similarly to (2.26)-(2.28) in Chapter 2, constraints (4.22)-(4.24) ensure that the travel plus expected inspection time along each route is no more than T_{Total}. Furthermore, constraints (4.22)-(4.24) eliminate subtours.

Finally, the third solution approach we consider extends the truncated knapsack orienteering problem defined in [45]. Specifically, we partition the total time budget into $T_{Total} = T_{travel} + T_{inspect}$. Then, we consider the problem of selecting a scheduling of operations that maximizes the expected reward from the inspected sites, with the added constraints that each team does not travel for more than T_{travel} units of time, and does not inspect for more than $T_{inspect}$ units of time in expectation. However, as mentioned in [45], associating to each site its expected inspection time does not

perform well in situations where the allowed inspection time $T_{inspect}$ does not permit the inspection of a site almost surely. As a consequence, the authors proposed to assign to each site its "truncated" inspection time $\sum_{s\geq 0}\min\{s, T_{inspect}\}f_i(s)$, and its associated reward, which in this case takes the form of $\sum_{k=1}^{n_i} v_i^k \pi_i^k \mathbb{P}(T_i^k \leq T_{inspect}) = \sum_{k=1}^{n_i} v_i^k \pi_i^k \sum_{s=0}^{T_{inspect}} f_i^k(s)$. We formulate the problem as follows:

$$\max \quad \sum_{i\in\mathcal{V}}\sum_{k=1}^{n_i} v_i^k \pi_i^k \sum_{s=0}^{T_{inspect}} f_i^k(s) \sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} x_{ji} \tag{4.25}$$

s.t. (4.19) − (4.21),

$$y_{s_0 j} = t_{s_0 j} x_{s_0 j}, \qquad \forall j \in \mathcal{V} \tag{4.26}$$

$$y_{ij} \leq T_{travel} x_{ij}, \qquad \forall (i,j) \in (\mathcal{V}\cup\{s_0\})\times\mathcal{V} \mid i \neq j \tag{4.27}$$

$$\sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} y_{ij} = \sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} y_{ji} + \sum_{\substack{j\in\mathcal{V}\\ j\neq i}} t_{ij} x_{ij}, \qquad \forall i \in \mathcal{V} \tag{4.28}$$

$$w_{s_0 j} = \sum_{s\geq 0} \min\{s, T_{inspect}\} f_j(s) x_{s_0 j}, \qquad \forall j \in \mathcal{V} \tag{4.29}$$

$$w_{ij} \leq T_{inspect} x_{ij}, \qquad \forall (i,j) \in (\mathcal{V}\cup\{s_0\})\times\mathcal{V} \mid i \neq j \tag{4.30}$$

$$\sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} w_{ij} = \sum_{\substack{j\in\mathcal{V}\cup\{s_0\}\\ j\neq i}} w_{ji} + \sum_{\substack{j\in\mathcal{V}\\ j\neq i}}\sum_{s\geq 0} \min\{s, T_{inspect}\} f_j(s) x_{ij}, \quad \forall i \in \mathcal{V} \tag{4.31}$$

$$x_{ij} \in \{0,1\}, \qquad \forall i \neq j \in \mathcal{V}\cup\{s_0\}$$

$$w_{ij}, y_{ij} \geq 0, \qquad \forall i \neq j \in \mathcal{V}\cup\{s_0\}.$$

Constraints (4.26)-(4.28) ensure that each team does not travel for more than T_{travel} units of time. Similarly, constraints (4.29)-(4.31) ensure that the total expected inspection time for each team, given the time limit $T_{inspect}$, does not exceed $T_{inspect}$ units of time.

However, one of the main challenges of this solution approach is to determine how to partition the total time into travel time and inspection time. Since we do not

know a priori the best partitioning, we solve the mixed-integer program (4.25)-(4.31) for $T_{inspect} = \ell \times 0.1 \times T_{Total}$, $\forall \ell \in [\![1, 10]\!]$, and keep the solution with the highest objective value.

4.4 Computational Study

We conduct a computational study involving 4000 randomly generated instances with a small number of sites and a single team, and we compare the solution approaches defined in Section 4.3. Figure 4-2 illustrates the performance of the approximation methods using regression error characteristic (REC) curves [19].

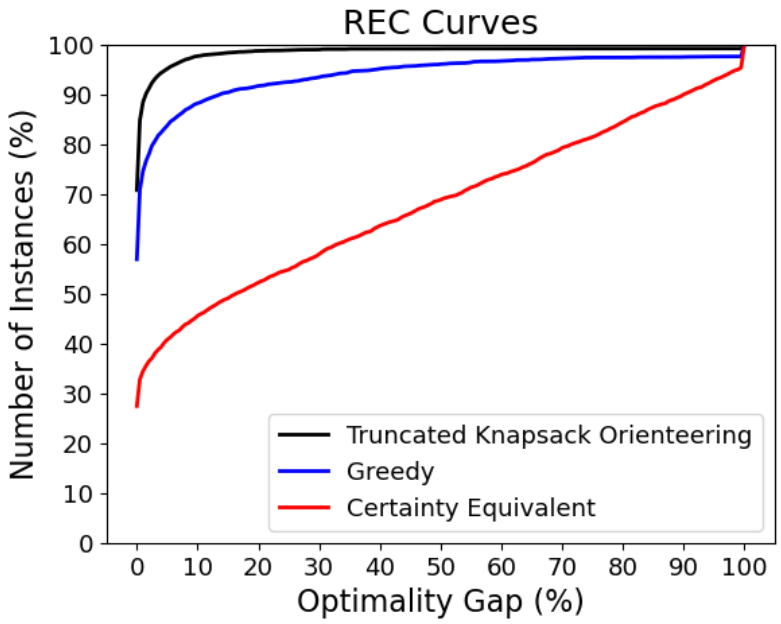


Figure 4-2: Performance of approximate solution approaches.

Specifically, Figure 4-2 shows on the $y-$axis the cumulative number of instances with an optimality gap upper bounded by the corresponding value on the $x-$axis. For instance, we find that for 88.3% of the instances, the greedy algorithm outputs a solution with an optimality gap less than 10%. In general, a method performs better as its REC curve shifts towards the top left corner of the plot.

From this figure, we first observe that the greedy algorithm (Algorithm 4) performs reasonably well; the average optimality gap is 5.83%. Interestingly, we observe that

the certainty equivalent formulation (4.18)-(4.24) performs poorly, with an average optimality gap of 31.91%. The main reason is that the solution generated by this approach fails to achieve the right tradeoff between the time that should be spent traveling and the time that should be spent inspecting. This motivates the third solution approach, which extends the truncated knapsack orienteering model from [45]. From Figure 4-2, we observe that solving the mixed-integer program (4.25)-(4.31) 10 times (for different partitionings of T_{Total} into $T_{travel} + T_{inspect}$) and keeping the best solution performs extremely well, with an average optimality gap of 1.39%. This computational study shows that the first and third solution approaches are viable options to compute scheduling of operations.

However, this computational study also demonstrates the value of computing the optimal scheduling of operations, whenever possible. Indeed, although the greedy algorithm and mixed-integer program (4.25)-(4.31) perform very well on average, there exist problem instances for which the optimality gap is large: As part of our randomly generated instances, we found instances for which the optimality gap of the solution generated by the greedy algorithm is 80%, and the optimality gap of the solution generated by (4.25)-(4.31) is 60%. For such instances, solving the mixed-integer programs (IP_1) and (IP_2) formulated in Section 4.3.1 (to optimally solve the PDIP) will significantly improve the scheduling of operations.

4.5 Summary

In this chapter, we studied the problem of optimal scheduling of inspection operations under imperfect diagnostic information regarding failure locations. We modeled this problem as a team orienteering problem with stochastic rewards and inspection times, and consists of finding a scheduling of sites to inspect that maximizes the expected reward obtained from successfully identifying failures in the network. To overcome the computational challenge in solving this NP-hard problem, we identified key features of optimal solutions to develop compact mixed-integer programming-based solution approaches, as well as approximate solution approaches. We compared these solu-

tion approaches using a computational study and found that our greedy algorithm and extension of the truncated knapsack orienteering problem perform very well on average. Nonetheless, our computational study also showed that solving our exact mixed-integer programming formulations significantly improves the scheduling of operations for some problem instances. Our approaches lead to practical strategies which prescribe an a priori response schedule. Importantly, they capture the essential trade-off between the travel time between sites and the inspection time of each site, given the imperfect diagnostic information, distances between sites, and available response time. These results demonstrate the advantages of integrating predictive models of failures into emergency response operations.

4.6 Proofs of Statements

Proof of Lemma 15. Consider a route $p_i = \{i_0, \ldots, i_{m_i}\} \in \mathcal{P}$, and let z^* be the quantity defined in (4.3). Then, trivially:

$$\forall t \in \mathbb{Z},\ z^*_{i_0}(t) = \mathbb{P}(0 \leq t) = \mathbb{1}_{\{t \geq 0\}}.$$

Furthermore:

$$\begin{aligned}
\forall l \in [\![1, m_i - 1]\!],\ \forall t \in \mathbb{Z},\ z^*_{i_l}(t) &\overset{(4.3)}{=} \mathbb{P}\Big(\sum_{j=1}^{l} T_{i_j} \leq t - \sum_{j=0}^{l-1} t_{i_j, i_{j+1}}\Big) \\
&= \sum_{s=0}^{t} f_{i_l}(s) \mathbb{P}\Big(\sum_{j=1}^{l-1} T_{i_j} \leq t - s - t_{i_{l-1}, i_l} - \sum_{j=0}^{l-2} t_{i_j, i_{j+1}}\Big) \\
&= \sum_{s=0}^{t - t_{i_{l-1}, i_l}} f_{i_l}(s) z^*_{i_{l-1}}(t - t_{i_{l-1}, i_l} - s).
\end{aligned}$$

□

Proof of Proposition 15. From constraints (4.7)-(4.9), we deduce that a feasible solution of (IP_1) consists of a scheduling of operations $(p_1, \ldots, p_b) \in \mathcal{A}$. Let us consider route p_i, with $i \in [\![1, b]\!]$, and let us express it as follows: $p_i = \{i_0 = s_0, i_1, \ldots, i_{m_i}, s_0\}$.

Then, the z variables along route p_i satisfy (from constraints (4.10)-(4.11)):

$$\forall t \in [\![0, T_{Total}]\!],\ z^t_{s_0 i_1} \leq 1,$$
$$\forall t \in [\![0, T_{Total}]\!],\ \forall l \in [\![1, m_i - 1]\!], z^t_{i_l i_{l+1}} \leq \sum_{s=0}^{t-t_{i_{l-1},i_l}} f_{i_l}(s) z_{i_{l-1} i_l}^{t-t_{i_{l-1},i_l}-s}$$

We then show by induction that $\forall t \in [\![0, T_{Total}]\!], \forall l \in [\![0, m_i - 1]\!],\ z^t_{i_l i_{l+1}} \leq z^*_{i_l}(t)$:

$$\forall t \in [\![0, T_{Total}]\!],\ z^t_{i_0 i_1} \overset{(4.10)}{\leq} 1 \overset{(4.4)}{=} z^*_{i_0}(t).$$

Now, let us assume that given $l \in [\![0, m_i - 2]\!],\ z^t_{i_l i_{l+1}} \leq z^*_{i_l}(t),\ \forall t \in [\![0, T_{Total}]\!]$. Then, we obtain:

$$\forall t \in [\![0, T_{Total}]\!],\ z^t_{i_{l+1} i_{l+2}} \leq \sum_{s=0}^{t-t_{i_l,i_{l+1}}} \underbrace{f_{i_{l+1}}(s)}_{\geq 0} z_{i_l i_{l+1}}^{t-t_{i_l,i_{l+1}}-s} \leq \sum_{s \geq 0} f_{i_{l+1}}(s) z^*_{i_l}(t - t_{i_l,i_{l+1}} - s)$$
$$\overset{(4.5)}{=} z^*_{i_{l+1}}(t).$$

This implies by induction that:

$$\forall t \in [\![0, T_{Total}]\!], \forall l \in [\![0, m_i - 1]\!],\ z^t_{i_l i_{l+1}} \leq z^*_{i_l}(t) \overset{(4.3)}{=} \mathbb{P}(\sum_{j=1}^{l} T_{i_j} \leq t - \sum_{j=0}^{l-1} t_{i_j, i_{j+1}}). \tag{4.32}$$

However, at optimality of (IP_1), inequality (4.32) will be tight, as the optimal solutions aim to maximize the $z_{ji}^{T_{Total}-t_{ji}-s}$ terms in the objective function. We can then conclude that the reward obtained for each site i_l visited along route p_i is indeed equal to the following:

$$\sum_{s=0}^{T_{Total}-t_{i_{l-1},i_l}} \sum_{k=1}^{n_{i_l}} v^k_{i_l} \pi^k_{i_l} f^k_{i_l}(s) z^*_{i_{l-1}}(T_{Total} - t_{i_{l-1},i_l} - s).$$

Now, we must ensure that subtours do not contribute any reward to the objective function. Assume that a feasible solution of (IP_1) contains a subtour $\{1, \ldots, m, m+$

$1 = 1\}$. From constraints (4.10) and (4.11), we deduce that:

$$\begin{aligned}
&\forall t \in [\![0, T_{Total}]\!],\ 0 \leq z_{m1}^t \leq \sum_{s_m=0}^{t-t_{m-1,m}} f_m(s_m) z_{m-1,m}^{t-t_{m-1,m}-s_m} \\
&\leq \sum_{s_m=0}^{t-t_{m-1,m}} \sum_{s_{m-1}=0}^{t-t_{m-1,m}-t_{m-2,m-1}-s_m} f_m(s_m) f_{m-1}(s_{m-1}) z_{m-2,m-1}^{t-t_{m-1,m}-t_{m-2,m-1}-s_m-s_{m-1}} \\
&\leq \sum_{s_m=0}^{t-t_{m-1,m}} \cdots \sum_{s_1=0}^{t-\sum_{j=1}^m t_{j,j+1}-\sum_{j=2}^m s_j} \left(\prod_{j=1}^m f_j(s_j)\right) z_{m1}^{t-\sum_{j=1}^m t_{j,j+1}-\sum_{j=1}^m s_j}. \qquad (4.33)
\end{aligned}$$

Next, we show by induction that $\forall t \in [\![0, T_{Total}]\!],\ z_{m1}^t = 0$. First, let us show that $z_{m1}^0 = 0$. If $\sum_{j=1}^m t_{j,j+1} > 0$, then a direct consequence of (4.33) is that $0 \leq z_{m1}^0 \leq 0$. If $\sum_{j=1}^m t_{j,j+1} = 0$, then (4.33) becomes:

$$0 \leq z_{m1}^0 \leq \underbrace{\left(\prod_{j=1}^m f_j(0)\right)}_{<1} z_{m1}^0,$$

since we assumed that each site requires a positive amount of inspection time with positive probability. As a consequence z_{m1}^0 must be equal to 0.

Now, let us select $t \in [\![0, T_{Total} - 1]\!]$, and let us assume that for every $t' \in [\![0, t]\!]$, $z_{m1}^{t'} = 0$. If $\sum_{j=1}^m t_{j,j+1} > 0$, then we also obtain from (4.33) and the inductive hypothesis that $0 \leq z_{m1}^{t+1} \leq 0$. Finally, if $\sum_{j=1}^m t_{j,j+1} = 0$, then (4.33) and the inductive hypothesis imply that:

$$0 \leq z_{m1}^{t+1} \leq \underbrace{\left(\prod_{j=1}^m f_j(0)\right)}_{<1} z_{m1}^{t+1}.$$

Thus, $z_{m1}^{t+1} = 0$.

Therefore, we proved by induction that $\forall t \in [\![0, T_{Total}]\!],\ z_{m1}^t = 0$. Then, by applying (4.11), we easily deduce that $\forall t \in [\![0, T_{Total}]\!],\ z_{12}^t = 0$. By repeating this process, we obtain that $\forall j \in [\![1, m]\!],\ \forall t \in [\![0, T_{Total}]\!],\ z_{j,j+1}^t = 0$.

Therefore, if a feasible solution to (IP_1) contains subtours, they do not contribute

to the objective function. Thus, if an optimal solution of (IP_1) contains subtours, we can remove the subtours from the solution and still maintain optimality.

□

Proof of Proposition 16. From constraints (4.13)-(4.15), we deduce that a feasible solution of (IP_2) consists of a scheduling of operations $(p_1, \ldots, p_b) \in \mathcal{A}$. Contrary to a feasible solution of (IP_1), a feasible solution to (IP_2) visits every site in $\mathcal{V}$ (potentially with a reward equal to 0). Let us consider route p_i, with $i \in [\![1, b]\!]$, and let us express it as follows: $p_i = \{i_0 = s_0, i_1, \ldots, i_{m_i}, s_0\}$. Then, the z variables along route p_i satisfy (from constraints (4.13)-(4.14),(4.16)-(4.17)):

$$\forall t \in [\![0, T_{Total}]\!],\ \forall l \in [\![1, m_i]\!],\ z^t_{i_l,k} \leq \sum_{s=0}^{t-t_{i_{l-1},i_l}} f^k_{i_l}(s) \sum_{k'=1}^{n_{i_{l-1}}} \pi^{k'}_{i_{l-1}} z^{t-t_{i_{l-1},i_l}-s}_{i_{l-1},k'}. \tag{4.34}$$

We show by induction that $\forall t \in [\![0, T_{Total}]\!]$, $\forall l \in [\![1, m_i]\!]$, $\forall k \in [\![1, n_{i_l}]\!]$, $z^t_{i_l,k} \leq \mathbb{P}(\sum_{j=1}^{l-1} T_{i_j} + T^k_{i_l} \leq t - \sum_{j=0}^{l-1} t_{i_j,i_{j+1}})$. For $l = 1$, we first obtain:

$$\forall t \in [\![0, T_{Total}]\!],\ \forall k \in [\![1, n_{i_1}]\!],\ z^t_{i_1,k} \overset{(4.16),(4.34)}{\leq} \sum_{s=0}^{t-t_{i_0,i_1}} f^k_{i_1}(s) = \mathbb{P}(T^k_{i_1} \leq t - t_{i_0,i_1}).$$

Now, let us consider $l \in [\![1, m_i - 1]\!]$ and let us assume that $\forall t \in [\![0, T_{Total}]\!]$, $\forall k \in [\![1, n_{i_l}]\!]$, $z^t_{i_l,k} \leq \mathbb{P}(\sum_{j=1}^{l-1} T_{i_j} + T^k_{i_l} \leq t - \sum_{j=0}^{l-1} t_{i_j,i_{j+1}})$. We then obtain:

$$\begin{aligned}
\forall t \in [\![0, T_{Total}]\!], \forall k \in [\![1, n_{i_{l+1}}]\!],\ z^t_{i_{l+1},k} &\overset{(4.34)}{\leq} \sum_{s=0}^{t-t_{i_l,i_{l+1}}} f^k_{i_{l+1}}(s) \sum_{k'=1}^{n_{i_l}} \pi^{k'}_{i_l} z^{t-t_{i_l,i_{l+1}}-s}_{i_l,k'} \\
&\leq \sum_{s=0}^{t-t_{i_l,i_{l+1}}} f^k_{i_{l+1}}(s) \sum_{k'=1}^{n_{i_l}} \pi^{k'}_{i_l} \mathbb{P}(\sum_{j=1}^{l-1} T_{i_j} + T^{k'}_{i_l} \leq t - t_{i_l,i_{l+1}} - s - \sum_{j=0}^{l-1} t_{i_j,i_{j+1}}) \\
&= \sum_{s=0}^{t-t_{i_l,i_{l+1}}} f^k_{i_{l+1}}(s) \mathbb{P}(\sum_{j=1}^{l} T_{i_j} \leq t - s - \sum_{j=0}^{l} t_{i_j,i_{j+1}}) \\
&= \mathbb{P}(\sum_{j=1}^{l} T_{i_j} + T^k_{i_{l+1}} \leq t - \sum_{j=0}^{l} t_{i_j,i_{j+1}}).
\end{aligned}$$

Therefore, we proved by induction that:

$$\forall t \in [\![0, T_{Total}]\!],\ \forall l \in [\![1, m_i]\!],\ \forall k \in [\![1, n_{i_l}]\!],\ z^t_{i_l,k} \leq \mathbb{P}(\sum_{j=1}^{l-1} T_{i_j} + T^k_{i_l} \leq t - \sum_{j=0}^{l-1} t_{i_j,i_{j+1}}). \tag{4.35}$$

Similarly to (IP_1), inequality (4.35) will be tight at optimality to (IP_2), as the optimal solutions aim to maximize the $z^{T_{Total}}_{i,k}$ terms in the objective function. We can then conclude that the reward obtained for each site i_l visited along route p_i is indeed equal to the following:

$$\sum_{k=1}^{n_{i_l}} v^k_{i_l} \pi^k_{i_l} \mathbb{P}(\sum_{j=1}^{l-1} T_{i_j} + T^k_{i_l} \leq T_{Total} - \sum_{j=0}^{l-1} t_{i_j,i_{j+1}}).$$

As in the proof of Proposition 15, the z variables ensure that subtours do not contribute any reward to the objective function. Thus, if an optimal solution of (IP_2) contains subtours, we can remove the subtours from the solution and still maintain optimality.

□

Chapter 5

Concluding Remarks

5.1 Overall Summary

This thesis focuses on the design of inspection and response operations to improve the resilience of critical infrastructure networks against failure events resulting from cyber-physical attacks and natural events.

In Chapter 2, we studied the generic problem of strategic network inspection, in which a defender (inspection agency) is tasked with detecting the presence of multiple attacks in the network. We addressed the question of determining a randomized inspection strategy with minimum number of detectors that ensures a target detection performance. This question can be formulated as a mathematical program with constraints involving the Nash equilibria of a large-scale strategic game between the defender and attacker. We developed a novel approach to construct an approximate equilibrium strategy profile of the game by utilizing solutions of minimum set cover and maximum set packing problems. This construction generalizes some of the previously known results in security games, and is applicable to a variety of settings such as urban patrolling, sensing of gas and water networks, and routing of small Unmanned Aircraft Systems for leak detection.

In Chapter 3, we studied the problem in which a routing entity sends its flow through the network while facing heterogeneous path transportation costs, and an interdictor simultaneously interdicts one or more edges while facing edge interdiction

costs. The router (resp. interdictor) seeks to maximize the value of effective (resp. interdicted) flow net the transportation (resp. interdiction) cost. We showed that the equilibrium properties of the game can be described using primal and dual solutions of a minimum-cost circulation problem. Our equilibrium analysis relied on a more general result on the existence of a probability distribution on a finite partially ordered set (poset) that satisfies a set of constraints involving marginal probabilities of the poset's elements and maximal chains. We positively answered this question by designing a combinatorial algorithm. Our results provide a new characterization of the critical network components in strategic settings.

In Chapter 4, we developed a prescriptive analytics framework for localizing network failures in the aftermath of a natural disaster. Given the diagnostic information provided by a failure prediction model, we considered a generic team orienteering problem with stochastic profits and service times. By leveraging the features of the problem, we derived compact mixed-integer programming formulations that compute optimal a-priori routing of the inspection teams. We also studied approximate solution approaches, and compared them using a computational study. Our results show the value of integrating predictive analytics for improving response operations.

The main modeling contribution of this thesis is the study of generic models that are applicable to various settings, such as urban patrolling, sensing of gas and water networks, and routing of small Unmanned Aircraft Systems for leak detection. To address the computational challenges arising from the combinatorial nature of the problems, we provided solution approaches based on lower dimensional representations. We showed optimality guarantees of our proposed solutions by deriving theoretical characterizations of the optimal ones. This required exploiting the interplay between linear programming duality, submodularity, network flows, and game theory. This lead to solutions that are scalable, accurate, and implementable in practice. Finally, we applied our framework to real-world infrastructure networks, such as water distribution, gas transmission, and transportation networks.

5.2 Future Work

5.2.1 Strategic Inspection of Heterogeneous Components

A future research question is to solve the inspection problem from Chapter 2 under a more refined detection model that accounts for imperfect detection of attacks (and other types of compromises). Typically, the diagnostic ability of sensing technology is represented by a probabilistic detection rate for any given false alarm rate. In fact, the guarantees provided by our approach can be easily extended (via simple scaling) to the case when the detection probability is a priori known and homogeneous across all detectors. The general case of heterogeneous detection rates can be addressed by extending our detection model; in particular, by adding a weight to each inspected node to represent the probability of detecting an attack within the node's monitoring set.

Finally, the question of how our solution approach can be extended to account for the heterogeneity of network components in terms of their criticality to the overall network functionality is also an interesting one. In principle, this case can be addressed by adding weights to the payoff functions of our defender-attacker game. However, in many practical situations, the defender can only qualitatively distinguish the criticality of various components (high versus low). In such cases, our approach for strategic network inspection can be applied to each group of components with homogeneous criticality levels, and the inspection strategies for individual groups can be then integrated based on the defender's operational constraints.

5.2.2 Strategic Interdiction of Multi-Commodity Network Flows

In Chapter 3, we studied a simultaneous game of full information between a malicious router and a security agency. One of the main modeling assumptions is that the problem's characteristics (network topology, transportation and interdiction costs) are common knowledge. However, in some situations, each player only has partial information about their adversary. We are interested in extending our work in this

direction, and addressing the following question: *How to design inspection operations for network interdiction under limited information?* We plan to answer this question by developing new ideas in adversarial multi-armed bandit problems and online optimization. In the exploration phase, the agency allocates interdiction resources to learn the preferences of the malicious router, who strategically responds to the agency's interdiction. In the exploitation phase, the agency utilizes the gained information to strategically allocate interdiction resources and optimally intercept the flow of malicious goods from the router. We would like to design policies that can improve the current inspection operations in uncertain and adversarial environment, and can directly benefit agencies addressing the security of critical infrastructure networks and supply chains. Applications of this work include strategic defense of critical food and drug delivery supply chains facing risks of adulteration and counterfeiting by adversarial entities.

Bibliography

[1] Ilan Adler and Renato D. C. Monteiro. A geometric view of parametric linear programming. *Algorithmica*, 8(1):161–176, Dec 1992.

[2] Mohamed Afif, Mhand Hifi, Vangelis Th. Paschos, and Vassilis Zissimopoulos. A new efficient heuristic for the minimum set covering problem. *The Journal of the Operational Research Society*, 46(10):1260–1268, 1995.

[3] Zakir Hussain Ahmed. A lexisearch algorithm for the distance-constrained vehicle routing problem. *International Journal of Mathematical and Computational Methods*, pages 165–174, 2016.

[4] Angeliki Aisopou, Ivan Stoianov, and Nigel J. D. Graham. In-pipe water quality monitoring in water supply systems under steady and unsteady state flow conditions: A quantitative assessment. *Water Research*, 46(1):235 – 246, 2012.

[5] Michael Allen, Ami Preis, Mudasser Iqbal, Seshan Srinangarajan, Hock B. Lim, Lewis Girod, and Andrew J. Whittle. Real time in-network monitoring to improve operational efficiently. *Journal - American Water Works Association*, 103(7):63–75, 2011.

[6] Mallik Angalakudati, Siddharth Balwani, Jorge Calzada, Bikram Chatterjee, Georgia Perakis, Nicolas Raad, and Joline Uichanco. Business analytics for flexible resource allocation under random emergencies. *Management Science*, 60(6):1552–1573, 2014.

[7] Sepehr Assadi, Ehsan Emamjomeh-Zadeh, Ashkan Norouzi-Fard, Sadra Yazdanbod, and Hamid Zarrabi-Zadeh. The minimum vulnerability problem. *Algorithmica*, 70(4):718–731, December 2014.

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

[9] U. Attorney. Sacramento man pleads guilty to attempting to shut down California's power grid. `http://www.usdoj.gov/usao/cae/press_releases/`.

[10] Rudolf Avenhaus and Morton John Canty. Inspection games. In Robert A. Meyers, editor, *Encyclopedia of Complexity and Systems Science*, pages 4855–4868. Springer, 2009.

[11] Michel Balinski and Albert W. Tucker. Duality theory of linear programs: A constructive approach with applications. *SIAM Review*, 11(3):347–377, 1969.

[12] Michael O. Ball, Bruce L. Golden, and Rakesh V. Vohra. Finding the most vital arcs in a network. *Operations Research Letters*, 8(2):73–76, April 1989.

[13] Melike Baykal-Gürsoy, Zhe Duan, H. Vincent Poor, and Andrey Garnaev. Infrastructure security games. *European Journal of Operational Research*, 239(2):469–478, 2014.

[14] C Berge and Pierre Duchet. Strongly perfect graphs. *Annals of Discrete Mathematics*, 21, 01 1984.

[15] Jonathan Berry, William Hart, Cynthia A. Phillips, James G. Uber, and Jean-Paul Watson. Sensor placement in municipal water networks with temporal integer programming models. *Journal of Water Resources Planning and Management*, 132(4):218–224, 2006.

[16] Dimitris Bertsimas, Ebrahim Nasrabadi, and James B. Orlin. On the power of randomization in network interdiction. *Operations Research Letters*, 44(1):114 – 120, 2016.

[17] Dimitris Bertsimas, Ebrahim Nasrabadi, and James B. Orlin. On the power of randomization in network interdiction. *Operations Research Letters*, 44(1):114 – 120, 2016.

[18] Dimitris Bertsimas, Ebrahim Nasrabadi, and Sebastian Stiller. Robust and adaptive network flows. *Operations Research*, 61(5):1218–1242, 2013.

[19] Jinbo Bi and Kristin P Bennett. Regression error characteristic curves. In *Proceedings of the 20th international conference on machine learning (ICML-03)*, pages 43–50, 2003.

[20] Gerald Brown, Matthew Carlyle, Javier Salmerón, and Kevin Wood. Defending critical infrastructure. *Interfaces*, 36(6):530–544, 2006.

[21] Saikat Chakrabarti, Elias Kyriakides, and Demetrios G. Eliades. Placement of synchronized measurements for power system observability. *Power Delivery, IEEE Transactions on*, 24(1):12–19, Jan 2009.

[22] Chee-Yee Chong and S. P. Kumar. Sensor networks: evolution, opportunities, and challenges. *Proceedings of the IEEE*, 91(8):1247–1256, Aug 2003.

[23] Vasek Chvatal. A greedy heuristic for the set-covering problem. *Mathematics of Operations Research*, 4(3):233–235, 1979.

[24] Kelly J. Cormican, David P. Morton, and R. Kevin Wood. Stochastic Network Interdiction. *Operations Research*, 46(2), 1998.

[25] Joseph R. Dancy and Victoria A. Dancy. Terrorism and oil & gas pipeline infrastructure: Vulnerability and potential liability for cybersecurity attacks. *oil and Gas, Natural Resources, and Energy Journal*, 2(6):579, 2017.

[26] George B. Dantzig and Philip Wolfe. Decomposition principle for linear programs. *Operations Research*, 8(1):101–111, 1960.

[27] Brian C. Dean, Michel X. Goemans, and Jan VondrÃąk. Approximating the stochastic knapsack problem: The benefit of adaptivity. *Mathematics of Operations Research*, 33(4):945–964, 2008.

[28] Ajay Deshpande, Sanjay E Sarma, Kamal Youcef-Toumi, and Samir Mekid. Optimal coverage of an infrastructure network using sensors with distance-decaying sensing quality. *Automatica*, 49(11):3351–3358, 2013.

[29] A. Dwivedi and X. Yu. A maximum-flow-based complex network approach for power system vulnerability analysis. *IEEE Transactions on Industrial Informatics*, 9(1):81–88, Feb 2013.

[30] David Eppstein. Parallel recognition of series-parallel graphs. *Information and Computation*, 98(1):41 – 55, 1992.

[31] R. Esposito. Hackers penetrate water system computers, Oct 2006. `http://blogs.abcnews.com/`.

[32] Nicolas Falliere, Liam Murchu, and Eric Chien. *W32.Stuxnet Dossier*. Symantec, 2010.

[33] Uriel Feige. On maximizing welfare when utility functions are subadditive. *SIAM Journal on Computing*, 39(1):122–142, 2009.

[34] Robert W. Floyd. Algorithm 97: Shortest path. *Commun. ACM*, 5(6):345–, June 1962.

[35] Drew Fudenberg and David K. Levine. *The Theory of Learning in Games*. EBSCO eBook Collection. MIT Press, 1998.

[36] DelbertR Fulkerson. Anti-blocking polyhedra. *Journal of Combinatorial Theory, Series B*, 12(1):50 – 71, 1972.

[37] Andrey Garnaev. *Search Games and Other Applications of Game Theory*. Lecture Notes in Economics and Mathematical Systems. Springer Berlin Heidelberg, 2000.

[38] Andrey Garnaev, G. Garnaeva, and P. Goutal. On the infiltration game. *International Journal of Game Theory*, 26(2):215–221, 1997.

[39] Orazio Giustolisi, Dragan Savic, and Zoran Kapelan. Pressure-driven demand and leakage simulation for water distribution networks. *Journal of Hydraulic Engineering*, 134(5):626–635, 2008.

[40] Peter Gleick. Water and terrorism. *Water Policy*, 8:481–503, 2006.

[41] Alan J. Goldman and Albert W. Tucker. Theory of linear programming. In Harold W. Kuhn and Albert W. Tucker, editors, *Linear Inequalities and Related Systems*, volume 38 of *Annals of Mathematics Studies 35*, pages 53–98. Princeton University Press, 1957.

[42] Assane Gueye and Vladimir Marbukh. A game-theoretic framework for network security vulnerability assessment and mitigation. In Jens Grossklags and Jean Walrand, editors, *Decision and Game Theory for Security*, pages 186–200, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[43] Assane Gueye, V.ladimir Marbukh, and Jean C. Walrand. Towards a metric for communication network vulnerability to attacks: A game theoretic approach. In Vikram Krishnamurthy, Qing Zhao, Minyi Huang, and Yonggang Wen, editors, *Game Theory for Networks*, pages 259–274, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[44] Qingyu Guo, Bo An, Yair Zick, and Chunyan Miao. Optimal interdiction of illegal network flow. In *Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence*, IJCAI'16, pages 2507–2513, 2016.

[45] Anupam Gupta, Ravishankar Krishnaswamy, Viswanath Nagarajan, and R. Ravi. Running errands in time: Approximation algorithms for stochastic orienteering. *Mathematics of Operations Research*, 40(1):56–79, 2015.

[46] Anupam Gupta, Viswanath Nagarajan, and Sahil Singla. Algorithms and adaptivity gaps for stochastic probing. In *Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete algorithms*, pages 1731–1747. SIAM, 2016.

[47] Magnús M. Halldórsson, Jan Kratochvíl, and Jan Arne Telle. Independent sets with domination constraints. *Discrete Applied Mathematics*, 99(1âĂŞ3):39 – 54, 2000.

[48] Xin He and Yaacov Yesha. Parallel recognition and decomposition of two terminal series parallel graphs. *Information and Computation*, 75(1):15 – 38, 1987.

[49] M. Hifi. A genetic algorithm-based heuristic for solving the weighted maximum independent set and some equivalent problems. *The Journal of the Operational Research Society*, 48(6):612–622, 1997.

[50] Chính T. Hoàng. Efficient algorithms for minimum weighted colouring of some classes of perfect graphs. *Discrete Applied Mathematics*, 55(2):133 – 143, 1994.

[51] Metro Evacuation Project Homepage. `http://www.spatial.cs.umn.edu/Project/metro-evac/`.

[52] Robert B. Jackson, Adrian Down, Nathan G. Phillips, Robert C. Ackley, Charles W. Cook, Desiree L. Plata, and Kaiguang Zhao. Natural gas pipeline leaks across washington, dc. *Environmental Science & Technology*, 48(3):2051–2058, 02 2014.

[53] B. Jansen, C. Roos, and T. Terlaky. The theory of linear programming:skew symmetric self-dual problems and the central path. *Optimization*, 29(3):225–233, 1994.

[54] M. D. Jolly, A. D. Lothes, S. Bryson, and L. Ormsbee. Research database of water distribution system models. *Journal of Water Resources Planning and Management*, 140(4):410–416, 2014.

[55] Imdat Kara. Arc based integer programming formulations for the distance constrained vehicle routing problem. In *3rd IEEE International Symposium on Logistics and Industrial Informatics*, pages 33–38, Aug 2011.

[56] Imdat Kara and Tusan Derya. Polynomial size formulations for the distance and capacity constrained vehicle routing problem. *AIP Conference Proceedings*, 1389(1):1713–1718, 2011.

[57] Anna R. Karlin and Yuval Peres. Game theory, alive. `http://www.stat.berkeley.edu/~sly/gtlect.pdf`, June 2016.

[58] Anna R. Karlin and Yuval Peres. *Game Theory, Alive*. American Mathematical Society, 2016.

[59] Narendra Karmarkar. A new polynomial-time algorithm for linear programming. *Combinatorica*, 4(4):373–395, Dec 1984.

[60] Dénes König. Gráfok és mátrixok. *Matematikai és Fizikai Lapok*, 38:116–119, 1931.

[61] Andreas Krause, Brendan McMahan, Carlos Guestrin, and Anupam Gupta. Robust submodular observation selection. *Journal of Machine Learning Research (JMLR)*, 9:2761–2801, December 2008.

[62] Andreas Krause, Ajit Singh, and Carlos Guestrin. Near-optimal sensor placements in gaussian processes: Theory, efficient algorithms and empirical studies. *J. Mach. Learn. Res.*, 9:235–284, June 2008.

[63] D. Kravets. Feds: Hacker disabled offshore oil platform leak-detection system, March 2009. `http://www.wired.com`.

[64] H. Kuchler and N. Buckley. Hackers shut down ukraine power grid. *Financial Times*, January 2016.

[65] F-Secure Labs. Blackenergy and quedagh: The convergence of crimeware and apt attacks, 2016.

[66] Gilbert Laporte, Martin Desrochers, and Yves Nobert. Two exact algorithms for the distance-constrained vehicle routing problem. *Networks*, 14(1):161–172, 1984.

[67] Gilbert Laporte, Yves Nobert, and S. Taillefer. A branch-and-bound algorithm for the asymmetrical distance-constrained vehicle routing problem. *Mathematical Modelling*, 9(12):857 – 868, 1987.

[68] Steven Link. Predictive earthquake damage modeling for natural gas distribution infrastructure, June 2018. MIT Thesis.

[69] Richard J. Lipton, Evangelos Markakis, and Aranyak Mehta. Playing large games using simple strategies. In *Proceedings of the 4th ACM Conference on Electronic Commerce*, EC '03, pages 36–41, New York, NY, 2003. ACM.

[70] Philip Marcelo. Over-pressurized gas lines caused the deadly explosions near boston, federal report says. *Time*, October 2018.

[71] Marios Mavronicolas, Vicky Papadopoulou, Anna Philippou, and Paul Spirakis. A network game with attackers and a defender. *Algorithmica*, 51(3):315–341, 2008.

[72] Patrick McGeehan and Matt Flegenheimer. East village gas explosion reveals problems in city's inspection system. *New York Times*, 2015.

[73] H. Brendan Mcmahan, Georey J Gordon, and Avrim Blum. Planning in the presence of cost functions controlled by an adversary. In *In ICML*, pages 536–543, 2003.

[74] Alan W. McMasters and Thomas M. Mustin. Optimal interdiction of a supply network. *Naval Research Logistics Quarterly*, 17(3):261–268, 1970.

[75] R. McMillan. `http://www.computerworld.com/s/article/9007751/Two_charged_with_hacking_LA_traffic_lights`.

[76] C. E. Miller, Albert W. Tucker, and R. A. Zemlin. Integer programming formulation of traveling salesman problems. *Journal of the ACM*, 7(4):326–329, October 1960.

[77] Viswanath Nagarajan and R. Ravi. Approximation algorithms for distance constrained vehicle routing problems. *Networks*, 59(2):209–214, 2012.

[78] John F. Nash. Equilibrium points in n-Person games. *Proceedings of the National Academy of Sciences of the United States of America*, 36(1):48–49, 1950.

[79] Malik S. Naureen, Ryan Collins, and Meenal Vamburkar. Cyberattack pings data systems of at least four gas networks, 2018. `https://www.bloomberg.com/news/articles/2018-04-03/day-after-cyber-attack-a-third-gas-pipeline-data-system-shuts`.

[80] Sebastian Neumayer, Gil Zussman, Reuven Cohen, and Eytan Modiano. Assessing the impact of geographically correlated network failures. In *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pages 1–6, Nov 2008.

[81] Noam Nisan, Tim Roughgarden, Eva Tardos, and Vijay V. Vazirani. *Algorithmic Game Theory*. Cambridge University Press, New York, NY, USA, 2007.

[82] James B. Orlin, Serge A. Plotkin, and Éva Tardos. Polynomial dual network simplex algorithms. *Mathematical Programming*, 60(1):255–276, Jun 1993.

[83] James B Orlin, Andreas S Schulz, and Rajan Udwani. Robust monotone submodular function maximization. *Mathematical Programming*, 172(1):505–537, 2018.

[84] Avi Ostfeld and Elad Salomons. Optimal layout of early warning detection stations for water distribution systems security. *Journal of Water Resources Planning & Management*, 130(5):377 – 385, 2004.

[85] Avi Ostfeld, James G. Uber, Elad Salomons, Jonathan W. Berry, William E. Hart, Cindy A. Phillips, Jean-Paul Watson, Gianluca Dorini, Philip Jonkergouw, Zoran Kapelan, Francesco di Pierro, Soon-Thiam Khu, Dragan Savic, Demetrios Eliades, Marios Polycarpou, Santosh R. Ghimire, Brian D. Barkdoll, Roberto Gueli, Jinhui J. Huang, Edward A. McBean, William James, Andreas Krause, Jure Leskovec, Shannon Isovitsch, Jianhua Xu, Carlos Guestrin, Jeanne VanBriesen, Mitchell Small, Paul Fischbeck, Ami Preis, Marco Propato, Olivier Piller, Gary B. Trachtman, Zheng Yi Wu, and Tom Walski. The battle of the water sensor networks (bwsn): A design challenge for engineers and algorithms. *Journal of Water Resources Planning and Management*, 134(6):556–568, 2008.

[86] Tife Owolabi. Nigerian militant group claims attack on oil pipeline in niger delta, 2016. `https://www.reuters.com/article/us-nigeria-oil-idUSKCN11Z0XE`.

[87] Lina Perelman, Jonathan Arad, Mashor Housh, and Avi Ostfeld. Event detection in water distribution systems from multivariate water quality time series. *Environmental Science & Technology*, 46(15):8212–8219, 2012.

[88] Lina Perelman, Morris L. Maslia, Avi Ostfeld, and Jason B. Sautner. Using aggregation/skeletonization network models for water quality simulations in epidemiologic studies. *Journal - American Water Works Association*, 100(6):122–133, 2008.

[89] Lina Perelman and Avi Ostfeld. Operation of remote mobile sensors for security of drinking water distribution systems. *Water Research*, 47(13):4217 – 4226, 2013.

[90] PG&E. Pipeline accident report: Pacific gas and electric company natural gas transmission pipeline rupture and fire. Technical report, National Transportation Safety Board, September 2010.

[91] Nathan G. Phillips, Robert Ackley, Eric R. Crosson, Adrian Down, Lucy R. Hutyra, Max Brondfield, Jonathan D. Karr, Kaiguang Zhao, and Robert B. Jackson. Mapping urban pipeline leaks: Methane leaks across boston. *Environmental Pollution*, 173:1 – 4, 2013.

[92] James Pita, Manish Jain, Janusz Marecki, Fernando Ordóñez, Christopher Portway, Milind Tambe, Craig Western, Praveen Paruchuri, and Sarit Kraus. Deployed armor protection: The application of a game theoretic model for security at the los angeles international airport. In *Proceedings of AAMAS '08*, pages 125–132, 2008.

[93] Ryan Porter, Eugene Nudelman, and Yoav Shoham. Simple search methods for finding a nash equilibrium. *Games and Economic Behavior*, 63(2):642 – 662, 2008. Second World Congress of the Game Theory Society.

[94] H. Donald Ratliff, G. Thomas Sicilia, and S. H. Lubore. Finding the n most vital links in flow networks. *Management Science*, 21(5):531–539, 1975.

[95] Michele Romano, Zoran Kapelan, and Dragan A. Savic. Automated detection of pipe bursts and other events in water distribution systems. *Journal of Water Resources Planning and Management*, 140(4):457–467, 2012.

[96] Mary-Ann Russon. Hackers hijacking water treatment plant controls shows how easily civilians could be poisoned. *International Business Times*, 2016.

[97] Lina Sela Perelman, Waseem Abbas, Xenofon Koutsoukos, and Saurabh Amin. Sensor placement for fault location identification in water networks: A minimum test cover approach. *Automatica*, 72:166 – 176, 2016.

[98] Rebecca Smith. Assault on california power station raises alarm on potential for terrorism. *Wall Street Journal*, 2015.

[99] Zhihua Song, Han Zhang, Wanfang Che, and Xiaobin Hui. Algorithm for distance constrained aerial vehicle routing problem: Based on minimum spanning tree and genetic computation. In *2015 11th International Conference on Computational Intelligence and Security (CIS)*, pages 5–9, Dec 2015.

[100] Ivan Stoianov, Lama Nachman, Sam Madden, and Timur Tokmouline. PIPENET a wireless sensor network for pipeline monitoring. In *Proceedings of the 6th International Conference on Information Processing in Sensor Networks*, IPSN '07, pages 264–273, New York, NY, USA, 2007. ACM.

[101] Kelly M. Sullivan and J. Cole Smith. Exact algorithms for solving a euclidean maximum flow network interdiction problem. *Networks*, 64(2):109–124, 2014.

[102] Wai Yuen Szeto. Routing and scheduling hazardous material shipments: Nash game approach. *Transportmetrica B: Transport Dynamics*, 1(3):237–260, 2013.

[103] Vasileios Tzoumas, Konstantinos Gatsis, Ali Jadbabaie, and George J. Pappas. Resilient monotone submodular function maximization. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pages 1362–1367, Dec 2017.

[104] University of Exeter. Centre for Water Systems, 2014. Accessed October 24, 2014, `http://emps.exeter.ac.uk/engineering/research/cws/resources/benchmarks/design-resiliance-pareto-fronts/data-files/`.

[105] USEPA. *EPANET 2.00.12*. U.S. Environmental Protection Agency, Cincinnati, Ohio, 2002. `http://www2.epa.gov/water-research/epanet`, Accessed: 2014-10-24.

[106] Vijay V. Vazirani. *Approximation Algorithms*. Springer-Verlag New York, Inc., New York, NY, USA, 2001.

[107] Visenti. `http://www.visenti.com/`, 2007. Accessed: 2015-04-14.

[108] Joseph C. von Fischer, Daniel Cooley, Sam Chamberlain, Adam Gaylord, Claire J. Griebenow, Steven P. Hamburg, Jessica Salo, Russ Schumacher, David Theobald, and Jay Ham. Rapid, vehicle-based identification of location and magnitude of urban natural gas pipeline leaks. *Environmental Science & Technology*, 51(7):4091–4099, 04 2017.

[109] John Von Neumann. A certain zero-sum two-person game equivalent to the optimal assignment problem. *Contributions to the Theory of Games*, 2:5–12, 1953.

[110] Jiangwen Wan, Yang Yu, Yinfeng Wu, Renjian Feng, and Ning Yu. Hierarchical leak detection and localization method in natural gas pipeline monitoring sensor networks. *Sensors*, 12(1):189–214, 2012.

[111] Alan Washburn and Kevin Wood. Two-person zero-sum games for network interdiction. *Operations Research*, 43(2):243–251, 1995.

[112] Alan Washburn and Kevin Wood. Two-person zero-sum games for network interdiction. *Operations Research*, 43(2):243 – 251, 1995.

[113] CDJ Waters. Expanding the scope of linear programming solutions for vehicle scheduling problems. *Omega*, 16(6):577 – 583, 1988.

[114] Richard Wollmer. Removing Arcs from a Network. *Operations Research*, 12(6):934–940, 1964.

[115] R. Kevin Wood. Deterministic network interdiction. *Mathematical and Computer Modelling*, 17(2):1 – 18, 1993.