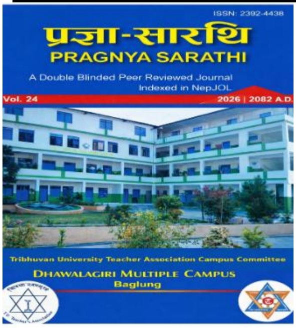
Publisher: TUTA, Dhawalagiri Multiple Campus, Baglung ISSN: 2392-4438



Article information

Received:	26 February 2026
Review:	1 March to 20 March 2026
Revision	21 March to 28 March 2026
Accept:	8 April 2026
Published:	15 April, 2026
DOI:	https://doi.org/10.3126/ps.v24i1.92763
Available:	www.nepjol.info/index.php/ps

A Survey on Robust Maximum Flow Network Interdiction Problem

Bishnu Prasad Chapagai[1*]
Dhawalagiri, Multiple Campus, TU
Email: chapagai15@gmail.com
*Corresponding author

Youb Raj Gaire[2]
Cantal Department of Mathematics, TU
Email: yrgaire01@gmail.com

Abstract

Network interdiction has become a vital topic in operations research and optimization. It examines how networked systems can be intentionally disrupted or affected by unforeseen disturbances. This paper presents a comprehensive overview of robust maximum flow interdiction problems that seek to restrict the maximum amount of flow an adversary can route through a network under uncertainty in network parameters. Additionally, the paper discusses various modeling approaches and solution techniques for these problems, highlighting their computational challenges and outlining promising directions for future research.

Keywords: bilevel programming, maximum flow, network interdiction, robust optimization, uncertainty

Introduction

Modern society depends on infrastructure that is built around networks – such as transportation, communication, electricity grids, water systems, and supply chains (Ahuja et al, 1993). Because these critical systems face risks from deliberate attacks, natural disasters, and accidental failure, researchers have put major effort into studying network interdiction problems. Fundamentally, these problems involve a strategic struggle between two opposing sides: the interdictor, who tries to disrupt how the network functions, and the operator or adversary, who tries to preserve or maximize the network's performance (Smith, 2011).

The maximum flow network interdiction problem first appeared in the 1960s in military and logistics setting (Wollmer, 1964), and over the past sixty years, it has seen significant progress. In this type of problem, an adversary aims to send as much flow as possible from source to a sink, while the interdictor tries to limit that flow by removing or blocking network arcs, subject to limited resources (Wood, 1993). The main challenge comes from the problem's two–level structure: the interdictor must anticipate the adversary's optimal response when selecting interdiction strategies.

A major step forward in the field has been the inclusion of uncertainty in the interdiction models. In real – life situations, decision – makers rarely have complete information about network parameters, such as arc capacities or how effective interdiction efforts will be (Chauhan et al., 2024). This uncertainty can stem from various sources, including limited intelligence about an adversary's capabilities, changing environmental conditions, measurement errors, and the inherent unpredictability of human behavior (Bertsimas et al., 2011).

This survey provides a systematic review of robust maximum flow network interdiction problems with four main objectives: (1) to develop a common framework for comparing different modeling approaches, (2) to summarize current solution techniques and finding on computational complexity, (3) to clarify how deterministic, stochastic and robust formulations relate to each other, and (4) to point out new research directions an unresolved question.

Literature Review

Origins of Network Interdiction

The study of network interdiction can be traced back to the mid in 1950s, when Harres and Ross (1955) explored vulnerabilities in the Soviet railway system. Their work relied on heuristic approaches to identify key bottlenecks that could significantly disrupt operations. Building on these early ideas, more structured and formal analyses began to appear in the early 1960s. In particular, Wollmer (1963) and Wollmer (1964) introduced algorithmic methods designed to determine which links in a railway network were most critical. These early works focused on military applications, particularly on interrupting enemy supply lines and communication networks during wartime (Dews & Kozaczka, 1981).

During the 1970s, theoretical progress accelerated, as researchers began exploring different types of interdiction goals and network configurations. McMasters and Mustin (1970) looked into how best to disrupt supply networks. While Ratliff et al. (1975) tackled the issue of identifying the most critical links in flow networks. Together, these studies helped establish a base for understanding the combinatorial difficulty inherent in interdiction problems.

The Max-Flow Min-Cut Theorem and Interdiction

The maximum flow interdiction problems rest on the theoretical base provided by the max – flow and min – cut theorem (Elias et al., 1956; Ford & Fulkerson, 1956). This theorem is important in the sense that it proves the maximum flow from the source to the sink is equivalent to the minimum cut from the source to the sink. This duality in the context of interdiction problems means that the interdictor aiming to reduce the maximum flow needs to target the arcs that would have the greatest impact on the minimum cut.

This relationship between cuts and interdiction strategies was exploited in the case of planar graphs in the seminal paper on the problem by Wollmer (1964), where the topological dual graphs were used to transform the interdiction problem into a shortest path problem on the expanded network.

Complexity Results

Wood (1993) was the first to give a comprehensive complexity result on the complexity of the maximum flow network interdiction problem; they showed that the problem is strongly NPhard when the network is directed, through a reduction from the clique problem. This showed that the cardinality-constrained problem of interdicting at most k arcs is also computationally hard. Phillips (1993) showed that the problem is NP-hard on planar graphs when the costs of interdiction are arbitrary, but only weakly NP-hard.

Altner et al. (2010) derived improved bounds on the approximability of maximum flow interdiction problems and showed their relationship to the R-interdiction covering problem. Chestnut and Zenklusen (2017) improved the results of Altner et al. (2010) by presenting approximation.

Problem Formulation and Modeling Paradigms

Deterministic Maximum Flow Interdiction

The deterministic maximum flow interdiction problem can be formulated as a bi-level optimization problem (Wood, 1993). Let $G = (N,A)$ be a directed graph with source node s and sink node t. Each arc $a \in A$ has a capacity u_a and an interdiction cost r_a. The interdictor selects a set of arcs to remove subject to a budget constraint $\sum_{\alpha \in A} r_a \, x_a \leq \Delta$, where $x_a \in \{0,1\}$ indicates whether arc a is interdicted. The adversary then solves a maximum flow problem on the residual network. The interdictor's objective is to minimize the resulting maximum flow value.

Wood (1993) demonstrated that this bilevel problem can be transformed into a single-level mixed-integer linear program using duality. Specifically, by taking the dual of the adversary's maximum flow problem (which becomes a minimum cut problem), the interdictor's problem becomes:

$$
\begin{aligned}
\min \quad & \textstyle\sum_{a\in A} u_a \beta_a \\
\text{s.t.} \quad & \textstyle\sum_{a\in A} r_a x_a \le \Delta \\
& \alpha_i - \alpha_j + \beta_a + x_a \ge 0 \quad \forall a = (i,j) \in A \\
& \alpha_s = 0, \alpha_t = 1 \\
& x_a \in \{0,1\}, \beta_a \in \{0,1\}, \alpha_i \in \{0,1\}
\end{aligned}
$$

where α variables represent the cut partition and β variables indicate forward arcs in the cut that are not interdicted.

Incorporating Uncertainty

The fact that the real-world interdiction problems are generally carried out under conditions of uncertainty has given rise to a number of modeling approaches, as explained by Bertsimas et al. (2011). They offer a detailed account of the theory of robust optimization and its applications. In the case of maximum flow interdiction, the conditions of uncertainty could be related to the capacities, costs, effectiveness, and behavior of the adversary.

Stochastic Programming Approaches

Cormican et al. (1998) proposed the concept of stochastic network interdiction, in which the success probability of network interdiction is incorporated. In this problem, the probability of
failure for the interdicted edges is given. The objective is to minimize the expected maximum flow. The problem can be formulated as follows:

$$\max_{x\in X} \mathbb{E}_\xi [\max_{y\in Y(x,\xi)} \mathrm{Val}(y)]$$

where ξ represents the random outcome of interdiction attempts. Janjarassuk & Linderoth (2008) developed decomposition and sampling methods for solving such problems, combining Benders decomposition with Monte Carlo sampling.

Robust Optimization with Uncertainty Sets

Chauhan et al. (2024) proposed a robust optimization framework for maximum flow interdiction under uncertainty in both arc capacities and interdiction resource consumption. Using the budgeted uncertainty approach of Bertsimas & Sim (2003, 2004), they assume that actual arc capacities lie in intervals $[u_{ij} - \widehat{u_{ij}}\ , u_{ij} +$

$\widehat{u_{ij}}$] and interdiction resource requirements lie in intervals $[r_{ij} - \widehat{r_{ij}}, r_{ij} + \widehat{r_{ij}}]$. The robust network interdiction problem (RNIP) is formulated as:

$$\begin{array}{ll} \min_\delta \max_{\gamma,\pi} & \min_x x_{ts} \\ \text{s.t.} & \sum_{(i,j)\in A} (r_{ij} + \hat{r}_{ij}\pi_{ij})\delta_{ij} \le \Delta \\ & \sum_{(i,j)\in A} \pi_{ij} \le \Pi, \quad \sum_{(i,j)\in A} \gamma_{ij} \le \Gamma \\ & \delta_{ij}, \gamma_{ij}, \pi_{ij} \in \{0,1\} \end{array}$$

where γ and π indicate which arcs realize worst-case capacity and resource consumption, respectively, and Γ and Π are budgets of uncertainty controlling the conservatism of the solution.

Solution Methodologies

Exact Methods

Dualize-and-Combine

The dualize-and-combine technique, first proposed in Wood (1993), still remains a key solution strategy to network interdiction problems. The dual of the follower's problem can be used to reduce the bilevel problem to a single-level optimization problem. However, the dualize-andcombine technique can be used if the follower's problem is convex and strong duality can be invoked, such as in maximum flow problems using the max-flow min-cut theorem and in shortest path problems. Israeli & Wood (2002) extended this approach to shortest path interdiction, demonstrating how dualization yields a mixed-integer linear program that can be solved by commercial solvers for modest-sized instances. The technique has been generalized to multicommodity flow interdiction by Lim & Smith (2007).

Benders Decomposition

Benders' decomposition has shown itself to be especially useful for network interdiction problems (Cormican, 1995; Wood, 2010). This method splits the overall problem into a master problem that handles interdiction choices and a set of sub-problems that assess the outcomes of those choices. In the context of maximum flow interdiction, the sub problem takes the form of a maximum flow calculation on the remaining network, which can be solved without much difficulty.

A thorough survey of Benders decomposition methods and their improvements can be found in Rahmaniani et al. (2017). Israeli & Wood (2002) put forward super-valid inequalities, which speed up convergence by removing integer solutions that cannot lead to a better objective value. Salmeron et al. (2009) adapted Benders decomposition to deal with nonconvex value functions in the context of electric power grid interdiction. More recently, Chauhan et al. (2024) proposed a heuristic based on Benders decomposition for the robust maximum flow interdiction problem, reporting reductions in computation time of over 90% relative to solving large test networks directly with mixed-integer programming (MIP).

Branch-and-Bound and Cutting Plane Methods

Several branch –and bound methods have been created to handle different types of interdiction problems. Granata et al. (2013) introduced a branch – and - price algorithm that combines column generation with branch and bound to solve the maximum flow network interdiction problem. Lonzno & Smith (2017) proposed a backward sampling technique that searches for the best interdiction strategy by enumerating the possible responses from the follower.

Heuristic Approaches

Lagrangian Relaxation

Lagrangian relaxation has been widely used in studying maximum flow interdiction problems. Early contributions by Bingol (2001) and Uygun (2002) showed that by relaxing some of the more complex constraints, the original problem can be separated into smaller and more manageable subproblems. Building on this idea, Royset and Wood (2007) integrated Lagrangian relaxation with a cut enumeration strategy to address interdiction models involving multiple objectives.

More recently, Chauhan et al. (2024) proposed a heuristic based on Lagrangian relaxation for the robust network interdiction problem (RNIP). Their method was able to produce strong upper bounds while significantly reducing computational effort, cutting solution time by more than 85% compared to traditional exact approaches.

Metaheuristics

Rocco and Ramirez–Marquez (2009) applied evolutionary algorithm techniques to deterministic network interdiction problems and found that these approaches perform effectively, particularly for networks of moderate size. Later, Michalopoulos and co-authors (2015) developed tabu search–based heuristics tailored to interdiction scenarios involving uncertain or covert smuggling operations. In a different application area, Khandzi and Sangaiah (2019) introduced genetic algorithm–based methods focused on safeguarding critical infrastructure in biomedical supply chains.

Machine Learning Approaches

Baycik (2022) explored how machine learning methods can be used to address maximum flow network interdiction problems. In this work, neural networks were trained to predict effective interdiction strategies by learning from structural and functional characteristics of the network. Building on this direction, Zhang and co-authors (2023) introduced a graph neural network–based framework, designed to handle interdiction tasks across different types of networks and varying problem scenarios.

Complexity and Approximability

Hardness Results

In general, the maximum flow interdiction problem is strongly NP-hard (Wood, 1993). However, several special cases admit polynomial-time algorithms:

Planar graphs with unit interdiction costs: Wollmer (1964) provided a polynomial algorithm using dual graph techniques.

Series-parallel graphs: Phillips (1993) developed pseudo-polynomial algorithms that can be converted to Fully Polynomial-Time Approximation Scheme (FPTAS). Unit capacity networks: Disser & Matuschke (2020) showed that robust maximum flow becomes polynomial when all arcs have unit capacity.

Single arc failure: Aneja et al. (2001) provided a polynomial algorithm for maximizing residual flow when one arc may fail.

Approximation Algorithms

Chestnut & Zenklusen (2017) presented approximation algorithms for maximum flow interdiction, achieving a $2(n-1)$-approximation in polynomial time. Boeckmann & Thielen (2021) developed a $(k+1)$-approximation for the k-most vital arcs problem, where the approximation ratio depends only on the number of removed arcs. Baffier & Suppakitpaisarn (2014) showed that maximum multiroute flows provide $(k + 1)$-approximations for the robust flow problem.

Specialized Algorithms for Robust Variants

Chauhan et al. (2024) developed three heuristics specifically for robust maximum flow interdiction:

Lagrangian Relaxation (LR): Breaks down the problem into four unconstrained optimisation problems and a maximum flow subproblem by relaxing the capacity resilience and resource consumption robustness requirements. Unboundedness is avoided via valid upper bounds determined from the problem structure.

Benders Decomposition-based Heuristic (BD): Partitions the problem by fixing capacity robustness variables, leading to a master problem with complexity similar to the original Robust Maximum Flow Network Interdiction Problem (RNIP). A simultaneous penalty heuristic solves the master problem efficiently.

Enhanced Benders Decomposition (EBD): Combines LR and BD by using LR solutions to initialize BD with better bounds and initial optimality cuts. EBD achieves final MIP gaps below 5% with computational time savings exceeding 90% compared to commercial MIP solvers.

Uncertainty Modeling in Maximum Flow Interdiction

Types of Uncertainty

Capacity Uncertainty

Arc capacities represent the maximum flow that can traverse a network element. In practice, capacities may be uncertain due to:

1. Weather conditions affecting transportation networks (Lam et al., 2008)
2. Variable equipment performance in communication networks
3. Adversary's ability to temporarily increase throughput
4. Measurement errors in data collection

Chauhan et al. (2024) modeled capacity uncertainty using symmetric intervals $[u_{ij}-\hat{u}_{ij}, u_{ij}+\hat{u}_{ij}]$, where the worst-case from the interdictor's perspective is the upper bound (more flow possible). Han et al. (2014) used uncertainty theory to model capacities as uncertain variables with no information on their probability distributions.

Interdiction Resource Uncertainty

The resources required to successfully interdict an arc may be uncertain due to: Variable adversary protection measures, weather or environmental conditions affecting interdiction operations, and incomplete intelligence about adversary capabilities

Bertsimas et al. (2016) considered randomized interdiction strategies in which the interdictor selects a probability distribution over arc sets, with the follower minimizing the expected flow. Holzmann & Smith (2019) examined shortest path interdiction with randomized strategies, showing that the problem becomes strongly NP-hard for nonlinear cost functions.

Interdiction Effectiveness Uncertainty

Even when resources are allocated, interdiction may not be completely successful. Cormican et al. (1998) modeled interdiction success probabilistically, with each interdicted arc failing independently with a given probability. Pan and Morton (2008) extended this idea to the interdiction of maximum-reliability paths, in which the follower aims to find the route with the greatest chance of evading detection.

Modeling Frameworks

Robust Optimization with Budgeted Uncertainty

The uncertainty budgeting method proposed by Bertsimas and Sim (2003, 2004) has found broad acceptance in the field of network interdiction. Their framework gives decision–makers a way to manage how conservative their choices are by using a parameter called Γ, or the uncertainty budget, which places a limit on the number of parameters that can differ from their usual values at the same time.

When applying this approach to maximum flow interdiction, Chauhan and Colleagues (2024) used two separate uncertainty budgets: one (Γ) for handling variations in arc capacities and another (Π) for addressing uncertainty in the resources required for interdiction. Under this robust formulation, the solution remains valid for any scenario where no more than Γ arcs hit their worst possible capacities and no more than Π interdicted arcs demand their highest possible resource levels.

Stochastic Programming

Stochastic programming methods rely on known probability distributions to represent uncertain parameters. Cormican and his team (1998) applied a scenario–based form of stochastic programming to handle uncertainty about whether interdiction efforts would succeed. Janjarassuk and Linderoth (2008) proposed sample average approximation techniques that create scenarios by drawing samples using Monte Carlo methods. Soleimani – Alyar and Ghaffari – Hadigheh (2018) examined network interdiction problems under uncertainty, in which arc capacities are treated as independent uncertain variables following either linear or zigzag patterns. They reformulated this problem as a bi-level mixed–integer optimization problem.

Distributionally Robust Optimization

Distributionally robust optimization serves as a middle group between stochastic and robust methods. It works on the assumption that the true probability distribution falls within a known range ot possibilities, called an ambiguity set. Sadana and Delage (2023) examined a distributionally robust, risk –average version of network interdiction, in which the interdictor aims to minimize the conditional value –at – risk while facing uncertainty about the underlying distribution. This type of approach guards against a lack of knowledge of the actual probability distribution, yet it avoids excessive conservatism often found in worst–case robust optimization.

Value of Robustness

A key issue in robust interdiction is whether explicitly accounting for uncertainty yields real advantages. Chauhan and Colleagues (2024) ran a series of detailed computational tests to compare outcomes from robust models against those from deterministic models that ignore uncertainty. Their Monte Carlo simulations produced several findings:

First, robust models give more accurate predictions of true maximum flow levels, showing errors below 6%, whereas deterministic models underestimate the true flow by at least 26% in a large network setting. Second, when interdiction resources are substantial (set at 15,000 units), robust choices cut the actual maximum flow by as much as 78% on average relative to the choices made by deterministic models. Third, the likelihood of successful interdiction rises notably, by about 38% when the interdiction budget is large, once uncertainty is taken into account. Taken together, these results indicate that robust optimization not only yields more dependable forecasts but also yields practically meaningful gains in the effectiveness of interdiction operations.

Comparative Analysis of Robust Flow Models

Path Model vs. Arc Model

Biefel et al. (2025) provided a detailed comparison of robust maximum flow models for scenarios in which arcs can fail. Two main approaches have gained prominence in the literature.

Path Model (PM)

In this model, flow is decomposed into s–t paths. If an arc fails, any flow traveling along paths that include that arc is completely lost. This model was first introduced by Aneja et al. (2001) for a single-arc failure, and later extended by Du & Chandrasekaran (2007) to handle multiple failures. Disser & Matuschke (2020) proved that the PM becomes strongly NP-hard when the number of failure arcs Γ is treated as part of the input; however, it remains solvable in polynomial time for Γ = 1.

Arc Model (AM)

In this model, flow is assigned directly to individual arcs. The key requirement is that weak flow conservation must hold at every node across all possible failure scenarios. Bertsimas et al. (2013) introduced AM and proved that it can be solved in polynomial time using linear programming. A notable drawback is that the solutions tend to be conservative because the model does not allow flow rerouting after arc failures.

General Model (GM)

Biefel et al. (2025) proposed a unifying GM to bridge the gap between the PM and AM. In this approach, flow is allocated to subpaths (path that may start and end at intermediate nodes). The GM captures key features of both PM and AM.

Flow on subpaths containing a failing arc is deleted (like PM)

Weak flow conservation must hold in every scenario (like AM)

GM contains PM and AM as special cases and yields less conservative solutions. Key complexity results include:

1. GM is polynomial for Γ = 1
2. GM is strongly NP-hard for arbitrary Γ
3. GM is polynomial when all arcs have unit capacity.
4. GM is NP-hard when capacities are in {1, ∞}

Solution Quality Comparisons

Biefel et al. (2025) established bounds on the gaps between models:

1. For any Γ, there exist instances where $f^*_{pm} > \alpha f^*_{am}$ for arbitrarily large α
2. For $\Gamma = 1$ on directed acyclic graphs, $f^*_{gm} \leq 2f^*_{pm}$ and $f^*_{am} \leq 2f^*_{pm}$
3. Conjecture: For general Γ, $f^*_{gm} \leq (\Gamma + 1)f^*_{pm}$ and $f^*_{am} \leq (\Gamma + 1)f^*_{pm}$

These results indicate that while AM provides computational tractability, it may significantly underestimate achievable robust flow, while GM offers a compromise between tractability and solution quality.

Price of Robustness

The price of robustness (Bertsimas & Sim, 2004) measures the loss in nominal optimal value required to achieve robustness. For maximum flow interdiction:

1. For $\Gamma = 1$, there exist optimal robust solutions that are also nominally optimal (Aneja et al., 2001; Biefel et al., 2025)
2. For $\Gamma \geq 2$, the price of robustness can be arbitrarily large for AM.
3. For PM and GM with $\Gamma \geq 2$, the price of robustness can be tuned by adjusting model parameters.

Dynamic and Time-Dependent Extensions

Flows Over Time

Flows over time (dynamic flows) incorporate transit times on arcs, and flow must reach the sink within a given time horizon T. Ford and Fulkerson (1958) introduced the concept of temporally repeated flows, showing that dynamic maximum flow can be reduced to static flow computation.

Robust Dynamic Flow Models

Gottschalk et al. (2018) studied robust flows over time where at most Γ arcs may be delayed. Their dynamic path model (DPM) assumes flow is assigned to paths, and delays affect entire paths containing delayed arcs. Key findings:

1. DPM is at least as hard as static PM
2. Temporally repeated flows are not optimal for DPM but satisfy certain approximation guarantees
3. For instance, satisfying the T-bounded path length property, optimal temporally repeated flows can be computed in polynomial time

Biefel et al. (2025) extended their general model to the dynamic setting, introducing:

1. Dynamic Arc Model (DAM): Polynomial-time solvable via linear programming
2. Dynamic General Model (DGM): Strongly NP-hard for arbitrary Γ

They also answered an open question from Gottschalk et al. (2018) by proving DPM is NP-hard even for $\Gamma = 1$, contrasting with the polynomial solvability of static PM for single arc failure.

Temporally Increasing Flows

Biefel et al. (2025) proposed temporally increasing flows as a heuristic for DGM, where flow on each sub path is non-decreasing over time. While not optimal in general, this concept provides a natural extension of temporally repeated flows and may yield approximation guarantees.

Game-Theoretic Perspectives

Stackelberg Games

The concept of network interdiction problems fits naturally within the framework of Stackelberg games (Von Stackelberg, 1952). In such a setting, a leader (interdictor) makes the first move, after which a follower (the adversary) responds optimally. And, a comprehensive survey of interdiction models and algorithms from a game theoretic perspective was provided by Smith and Song (2020).

Defender–Attacker–Defender Models

The defender–attacker–defender (DAD) model was proposed by Brown et al. (2006) to safeguard critical infrastructure. This unfolds the following three-stage game: in the first stage, the defender fortifies network components; in the second stage, the attacker interdicts a set of components subject to a budget; and in the third stage, the defender operates the residual network optimally.

Smith et al. (2007) developed bilevel and trilevel mathematical programs for designing networks that remain functional after interdiction attacks. Lozano and Smith (2017) proposed a backward sampling method to solve the DAD problems using bounds derived from both perceived and actual damage to uniform fortification choices.

Simultaneous Games and Nash Equilibrium

Washburn and Wood (1995) studied two-person zero-sum games and applied them to network interdiction, where both players act at the same time. In their model, the evader chooses a route to minimize the chance of being detected while the interdictor distributes monitoring resources. They demonstrated that a mixed strategy Nash equilibrium exists and can be obtained through linear programming. Goldberg (2017) extended this to non-zero-sum games with multiple origin-destination pairs and non-linear detection-probability functions. He proved that Nash equilibrium still exists and, under certain conditions, can be computed in polynomial time.

Information Asymmetry and Deception

Bayrak and Bailey (2008) studied shortest-path interdiction under asymmetric information, in which the follower operates with inaccurate cost perceptions that the leader knows about. This situation leads to bi-level formulations where the leader aims to drive up the follower’s actual cost, while the follower makes decisions based on its own incorrect understanding of the situation. Salmeron (2012) looked at deception tactics in network interdiction, like include using decoys or concealing defensive actions to mislead the attacker. Zheng and Castanon (2023) examined dynamic network interdiction games with imperfect information and deceptive elements. They modeled how the attacker updates its beliefs over time using a Partially Observable Markov Decision Process (POMDP). Later, Borrero et al. (2015) studied sequential shortest path interdiction under incomplete information. In their setup, the leader learns about the follower’s parameters through repeated interactions. Their approach uses a greedy yet robust policy that balances trying new actions (exploration) with sticking to known good ones (exploitation). Over time, this policy converges to a performance level that matches cases where both sides have perfect information.

Applications and Case Studies

Critical Infrastructure Protection

Researchers have made extensive use of network interdiction models to safeguard critical infrastructure. In a pair of studies, Salmeron and et al. (2004, 2009) looked at how the power grid could be made more secure against possible terrorist attacks. They developed two-level optimization models to pinpoint weak spots and plan defensive actions. Around the same time, Motto et al. (2005) formulated mixed integer programming methods for analyzing power system security. Yuan et al. (2016) studied and explored a robust optimization approach for making distribution networks more resilient to natural disasters, relying on defender–attacker–defender models. Ding et al. (2018) then introduced a two-stage robust optimization framework with multiple uncertainty sets to help protect the power system.

Counter terrorism and Border Security

Morton et al. (2007) developed a model aimed at stopping nuclear materials from being smuggled across borders with a focus on where to place sensors for the best chance of detection. Pan et al. (2003) formulated a stochastic program for intercepting smuggled nuclear material, while Sullivan et al. (2014) extended this work to border security under asymmetric information, where smugglers may have different perceptions of interdiction effectiveness. Zhang et al. (2018) studied the stochastic shortest path version of network interdiction, applying it to border security along the Arizona-Mexico boundary. This model accounted for how smugglers choose routes when they are not sure where interdiction efforts will be located.

Drug Trafficking Interdiction

Steinrauf (1991) applied network interdiction models to the cocaine trade in Bolivia, analyzing both road and river transport networks. Magliocca et al. (2019) took a different approach using agent-based modeling with 14 years of data to simulate how cocaine traffickers adjust their behavior in response to counterdrug operations. Chauhan (2020) developed robust maximum flow interdiction models for illegal drug networks. These models accounted for uncertainties in two key areas: arc capacities and resource consumption. According to computational experiments, robust decisions reduced actual drug flows by as much as 78% compared to deterministic methods.

Cyber Security and Communication Networks

Fu and Modiano (2019) studied network interdiction through the lens of adversarial traffic flows, modeling of service attacks where attackers send large amounts of traffic to eat up network resources. Sanjab et al. (2017) applied prospect theory to the cyber-physical security of drone delivery systems, creating network interdiction games that factor in human decision-making biases. Borndorfer et al.

(2016) examined optimal toll control as an extended form of network interdiction where authorities set tolls to shape traffic patterns.

Public Health and Epidemiology

Assimakopoulos (1987) applied the network interdiction model to infection control in hospitals, identifying critical pathways through which diseases spread. Nandi and Medal (2016) developed methods for removing links in contact networks to minimize the spread of infections. Recently, Kosmas et al. (2024) studied a multi-period maximum flow network interdiction model aimed at disrupting domestic sex trafficking networks, paying special attention to how these networks restructure over time.

Computational Challenges and Empirical Insights

Benchmark Instances and Test Networks

In the study of the network interdiction problem, computational studies employ random methods to generate networks with controlled parameters. The grid-based test network was introduced by Bingol (2001), where nodes are arranged in $n_1 \times n_2$ grids with diagonal connections. Chauhan et al. (2024) used a generator to create a test network of size 50×50 (with 2502 nodes and 9803 arcs) to 500×500 (with 250000 nodes and 998003 arcs). Key instance characters included in the Network are:

(1) Nominal capacities – randomly generated between 10 and 100 units.
(2) Capacity deviations – between 10% to 30% of nominal values.
(3) Interdiction resource – typically set 100 units per arc.
(4) Uncertainty budgets (Γ, , Π) – in controlling conservation levels.

Performance of Solution Methods

Chauhan et al. (2024) applied extensive computational experiments comparing three heuristics, LR, BD, and EBD, against the commercial solver Gurobi on 31 test networks.

Gurobi: Found optimal for all 50×50 networks, but solved only one of 10100 and 200200 networks optimally within 6 hours, and failed to find an initial solution for 500×500 networks in 12 hours.

LR: Strong upper bound (within 1.44% of optimal) but weak lower bound (gap upto 13.17%) and achieved 86–98%.

BD: Quality solution and sometimes worse than LR but 92–99% time saving and moderate gap 1.58–5.13%.

EBD: 90-99%-time savings, best compromise with gaps below 5%, combined strength of LR (solution quality) and BD (solution confidence). All heuristics obtained first solutions within 100 seconds even for the largest networks, making them suitable for time-sensitive applications.

Sensitivity Analysis: Sensitivity analyses make important insights about the robust interdiction models.

Amount of uncertainty: Chauhan et al. (2024) varied capacity and assure the resource deviations on normal values be 10%-30% (low) to 30%-90%(high). Surprisingly, robust models performed better with high uncertainty than low uncertainty, as uncertainty budgets provide more protection when deviations are larger.

Budget of uncertainty (Γ): Increasing Γ from 20 to 40 increased calculated maximum flow by 2% for 50×50 networks (0.4% for 500×500) without affecting actual flows or interdiction success rates.

Budget of resource uncertainty (Π): Increasing Π from 2 to 10 increased interdiction success rates from 56% to 78% and substantially reduced actual maximum flows, demonstrating the importance of accounting for resource consumption uncertainty.

Interdiction budget (Δ): Larger interdiction budgets (10,000-15,000 units) amplified the value of robustness, with robust decisions reducing actual flows by 78% for 50 × 50 networks compared to deterministic decisions.

Future Research Directions

Theoretical Open Problems

Several fundamental questions remain unresolved in robust maximum flow interdiction:

Complexity for fixed Γ: Disser and Matuschke (2020) showed the path model is NP-hard when Γ is part of the input, but complexity for fixed Γ ≥ 2 remains open. This question extends to the general model as well.

Gap bounds: Conjecture 3.12 of Biefel et al. (2025) posits that$f_{gm}^{*} \leq (\Gamma + 1) f_{gm}^{*}$ for all instances. Proving this would establish tight approximation bounds for the general model.

Integral flows: The complexity of integral versions of the arc model remains unclear, while Disser and Matuschke (2020) established NP-hardness for integral path model with Γ = 2 and capacities ≤ 3.

Time-dependent bounds: In dynamic settings, it remains unknown whether lower bounds on the price of robustness can depend on the time horizon T beyond the Γ+1 bound established for static cases.

Algorithmic Extensions

Exact algorithms for general graphs: While heuristics achieve excellent performance, developing exact algorithms that scale to very large networks remain challenging. And, the improved cutting plane method and branch and cut algorithm helps for further research.

Machine learning integration: Baycik (2022) demonstrated potential for machine learning in interdiction situation. On the work, there could be develop neural network architecture that learn to predict optimal interdiction strategies or generate the high quality initial solutions for exact method.

Distributed and parallel computing: Rahmaniani et al. (2017) demonstrates the benders decomposition that lends itself parallel implementation. And, as the extension, the real time interdiction for dynamic network could be established.

Temporally increasing flows: Biefel et al. (2025) introduced the temporally increasing flows for dynamic robust flows but the efficient algorithm for computing optimal temporally increasing flows and establishing approximation of it, is remain open to solve.

Model Extensions

Multi-commodity flows: Most of research on interdiction focuses on single-commodity flows. And, extending robust formulations to multi-commodity settings presents significant challenges due to coupling across commodities and increased complexity (Lim & Smith, 2007).

Multi-period and dynamic games: Real-world interdiction involves repeated interactions over time. In the area, Enayaty Ahangar et al. (2019) developed logic-based decomposition for multi-period network interdiction, but robust and adaptive formulations remain largely unexplored.

Endogenous uncertainty: In many applications, interdiction decisions affect the distribution of future uncertainties. Goel and Grossmann (2006) studied stochastic programs with decision-dependent uncertainty. And, the similar concepts could enrich robust interdiction models.

Interdependent infrastructures: Critical infrastructure systems rarely operate in isolation. For example, power grids often rely on communication networks to function properly, creating complex interdependencies. Capturing these relationships through multilayer network interdiction models is an important but still developing area of research.

Emerging Applications

Climate Resilience: With extreme weather events becoming more frequent, network interdiction models offer a way to spot weak points in transportation, power and water systems. This information can then guide decisions about where to invest in climate adaptation measures.

Cyber Physical System Security: When cyber and physical components are integrated, new opportunities for attacks emerge. Etasami and Basar (2019) review how dynamic games apply to cyber-physical security by pointing to several openings for interdiction-based modeling.

Pandemic Response: Ideas from network interdiction can help shape public health strategies. These include limiting disease spread through travel bans, quarantine policies and deciding how to allocate medical resources.

Autonomous Systems: As autonomous vehicles and drones become more common, they introduce new interdiction problems. Unlike traditional targets, these involve moving objects and networks that change over time.

Conclusion

The article presents the development of robust maximum flow network interdiction problems in a clear chronological order, offering a broad look at how the field has grown. It shows a clear shift from early military focused applications to today’s more complex models that account for various forms of uncertainty.

The main contributions from the literature can be grouped as follows:

Theoretical Foundation: Researchers have established complexity results that confirm how hard interdiction problems generally are. At the same time, they have identified special cases that remain manageable such as planar, graphs, unit networks and scenarios with only a single failure.

Modeling Frameworks: In this paper, several modeling frames are discussed in several distinct ways such as classic bilevel formulation, stochastic programming that handles scenario based uncertainty, robust optimization using budgeted uncertainty and distributionally robust approaches that offer a complementary way to capture real world unpredictability.

Solution Methods: Two broad categories of methods appear in the literature. Exact approaches like dualization, Benders decomposition and branch and bound are used alongside heuristic methods including Lagrangian relaxation, mataheuristic and machine learning. Together, they allow researchers to solve instances ranging from small to large and with different structural features.

Practical Relevance: The models have been applied to a wide range of real world problems, such as protecting critical infrastructure, counterterrorism, intercepting drug trafficking, cybersecurity and public health. This shows how broadly useful interdiction models have become.

Emerging Directions: Current work points several new research paths, dynamic flows, game theoretic extensions, multilayer networks and the integration of machine learning. The field of robust maximum flow interdiction continues to advance, driven both by theoretical progress and by pressing practical needs. As infrastructure becomes more interconnected, threats grow more significant, making these models and methods essential for building system resilience and supporting strategic decisions under uncertainty.

Ethical approval for the research: Not applicable

Consent for publication: Not applicable

Conflict of interest: The author does not have any conflict of interest with any institutions concerning this research

Ethical conduct of research: This paper is written ethically

References

Ahuja, R. K., Magnanti, T. L., & Orlin, J. B. (1993). *Network flows: Theory, algorithms, and applications*. Prentice Hall.

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

Aneja, Y. P., Chandrasekaran, R., & Nair, K. P. K. (2001). Maximizing residual flow under arc destruction. *Networks, 38*(4), 194–198.

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

Baffier, J.-F., & Suppakitpaisarn, V. (2014). A (k + 1)-approximation robust network flow algorithm and a tighter heuristic method using iterative multiroute flow. In S. Chakraborty, D. Kundu, & N. Sadagopan (Eds.), *Algorithms and computation: WALCOM 2014* (Lecture Notes in Computer Science, Vol. 8344, pp. 68–79). Springer.

Baycik, N. O. (2022). Machine learning based approaches to solve the maximum flow network interdiction problem. *Computers & Industrial Engineering, 167*, 107873.

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

Bertsimas, D., Brown, D. B., & Caramanis, C. (2011). Theory and applications of robust optimization. *SIAM Review, 53*(3), 464–501.

Bertsimas, D., Nasrabadi, E., & Orlin, J. B. (2016). On the power of randomization in network interdiction. *Operations Research Letters, 44*(1), 114–120.

Bertsimas, D., Nasrabadi, E., & Stiller, S. (2013). Robust and adaptive network flows. *Operations Research, 61*(5), 1218–1242.

Bertsimas, D., & Sim, M. (2003). Robust discrete optimization and network flows. *Mathematical Programming, 98*(1–3), 49–71.

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

Biefel, C., Kuchlbauer, M., Liers, F., & Waldmüller, L. (2025). Robust static and dynamic maximum flows. *Journal of Combinatorial Optimization, 49*(5), 78.

Bingol, L. (2001). *A Lagrangian heuristic for solving a network interdiction problem* (Master's thesis). Naval Postgraduate School.

Boeckmann, J., & Thielen, C. (2021). A (B + 1)-approximation for network flow interdiction with unit costs. *Discrete Applied Mathematics*.

Borndörfer, R., Sagnol, G., & Schwartz, S. (2016). An extended network interdiction problem for optimal toll control. *Electronic Notes in Discrete Mathematics, 52*, 301–308.

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

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

Chauhan, D. R. (2020). *Robust maximum flow network interdiction problem* (Master's thesis). Portland State University.

Chauhan, D., Unnikrishnan, A., Boyles, S. D., & Patil, P. N. (2024). Robust maximum flow network interdiction considering uncertainties in arc capacity and resource consumption. *Annals of Operations Research*, 1–37.

Chestnut, S. R., & Zenklusen, R. (2017). Hardness and approximation for network flow interdiction. *Networks, 69*(4), 378–387.

Cormican, K. J. (1995). *Computational methods for deterministic and stochastic network interdiction problems* (Master's thesis). Naval Postgraduate School.

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

Dews, E., & Kozaczka, F. (1981). *Air interdiction: Lessons from past campaigns*. RAND Corporation.

Ding, T., Yao, L., & Li, F. (2018). A multi-uncertainty-set based two-stage robust optimization to defender–attacker–defender model for power system protection. *Reliability Engineering & System Safety, 169*, 179–186.

Disser, Y., & Matuschke, J. (2020). The complexity of computing a robust flow. *Operations Research Letters, 48*(1), 18–23.

Du, D., & Chandrasekaran, R. (2007). The maximum residual flow problem: NP-hardness with two-arc destruction. *Networks, 50*(3), 181–182.

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

Enayaty-Ahangar, F., Rainwater, C. E., & Sharkey, T. C. (2019). A logic-based decomposition approach for multi-period network interdiction models. *Omega, 87*, 71–85.

Etesami, S. R., & Başar, T. (2019). Dynamic games in cyber-physical security: An overview. *Dynamic Games and Applications*.

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

Ford, L. R., & Fulkerson, D. R. (1958). Constructing maximal dynamic flows from static flows. *Operations Research, 6*, 419–433.

Fu, X., & Modiano, E. (2019). Network interdiction using adversarial traffic flows. In *IEEE INFOCOM 2019* (pp. 1765–1773). IEEE.

Goel, V., & Grossmann, I. E. (2006). A class of stochastic programs with decision-dependent uncertainty. *Mathematical Programming, 106*(2), 355–394.

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

Gottschalk, C., Koster, A. M., Liers, F., Peis, B., Schmand, D., & Wierz, A. (2018). Robust flows over time: Models and complexity results. *Mathematical Programming, 171*(1), 55–85.

About Authors

Bishnu Prasad Chapagain is currently affiliated with Dhawalagiri Multiple Campus, Tribhuvan University. His research focuses on optimization, graph theory, and interdiction problems. He has authored and co-authored several research papers, demonstrating his significant contributions to academic literature.

Yubaraj Gaire is affiliated with the Central Department of Mathematics, Tribhuvan University. His research interests include network optimization and maximum flow problems. He has authored and co-authored more than a dozen university-level mathematics textbooks and research articles, reflecting his significant contributions to mathematical research and academic literature.