Resilient and Distributed Discrete Optimal Transport with Deceptive Adversary: A Game-Theoretic Approach

Jason Hughes and Juntao Chen

***Abstract*— Optimal transport (OT) is a framework that can be used to guide the optimal allocation of a limited amount of resources. The classical OT paradigm does not consider malicious attacks in its formulation and thus the designed transport plan lacks resiliency to an adversary. To address this concern, we establish an OT framework that explicitly accounts for the adversarial and stealthy manipulation of participating nodes in the network during the transport strategy design. Specifically, we propose a game-theoretic approach to capture the strategic interactions between the transport planner and the deceptive attacker. We analyze the properties of the established two-person zero-sum game thoroughly. We further develop a fully distributed algorithm to compute the optimal resilient transport strategies, and show the convergence of the algorithm to a saddle-point equilibrium. Finally, we demonstrate the effectiveness of the designed algorithm using case studies.**

***Index Terms*— Discrete Optimal Transport, Distributed Algorithm, Adversarial Attack, Resilience, Resource Matching**

I. Introduction

OPTIMAL transport (OT) is a centralized framework that can be leveraged to design efficient resource distribution and matching schemes [1], [2]. The OT framework captures heterogeneous constraints between the resource suppliers and receivers and it has been used in various applications, such as the distribution of raw materials to manufacturers, dispatching of power restoration facilities in disaster affected neighborhoods, and matching between employees and tasks in an organization.

Under the standard OT paradigm, the planner designs the resource allocation scheme that maximizes the aggregated utility of all participants [3], [4]. The classical framework does not consider that the resource suppliers and receivers could be compromised by an attacker whose goal is to disrupt the resource allocation efficiency. To this end, our goal is to develop a more robust transport strategy by using a game-theoretic framework [5] that captures the interactions between the transport planner and the adversary. Specifically, the planner designs the transport plan that maximizes the social utility by anticipating the compromise of a set of participating nodes by the adversary. In comparison, the attacker's objective is to minimize the aggregated utility of all the nodes under the transport plan. The attacker is stealthy as it will not modify the node's preference information in an arbitrary manner but considers threshold and magnitude constraints during decision-making. The considered scenario is related to the resilient resource allocation under adversarial attacks in literature, including jamming attack [6], network topology attack [7], and data falsification attack [8].

The transport network becomes more complex with a growing number of participants, which can be observed from real-world applications. This large-scale feature of the OT problem gives rise to another concern on the centralized computation of the optimal transport scheme. The required computation for centralized planning grows exponentially with the number of participants in the framework. Thus, our goal is to develop a distributed algorithm for resilient optimal transport such that the centralized planner is not necessary. We leverage alternating direction method of multipliers (ADMM) technique [9] to achieve the distributed transport strategy design. One feature of the designed ADMM-based distributed algorithm is that each participant only needs to solve its own problem and exchange the results with the corresponding connected agents, which enables parallel updates on the transport solution.

We further develop a best response type of algorithm to account for the strategic attacks and focus on the scenarios when a set of targets (i.e., resource receivers) are compromised. Thus, in the algorithm, each deceptive target determines its resource requests from the connected source nodes and its manipulations on the preference data. During the iterative update, each target in the network proposes either a truthful solution or an adversarial solution depending on whether the target node is attacked. Comparatively, the source nodes' goal of maximizing their utility do not respond to the attacks directly but in an implicit manner when computing the transport strategy. This feature can be observed in the designed resilient algorithm.

The contributions of this paper are summarized as follows.

1) We establish an adversarial discrete optimal transport framework using a game-theoretic approach that captures the strategic interactions between the resource planner and the attacker.
2) We develop an ADMM-based distributed algorithm for computing the optimal transport strategies in the adversarial environment, where the obtained strategy is resilient to the attacks.
3) We show the convergence of the proposed distributed algorithm to a saddle-point equilibrium solution of the established game, and corroborate the algorithm using

The authors are with the Department of Computer and Information Sciences, Fordham University, New York, NY, 10023 USA. E-mail: {jhughes50,jchen504}@fordham.edu. This research was supported in part by a Faculty Research Grant from Fordham Office of Research.

case studies.

The rest of the paper is organized as follows. Section II formulates a general adversarial OT framework for resource matching. Section III presents a class of adversarial OT problem with linear utilities. Section IV develops a distributed algorithm to compute the resilient optimal transport strategy. Section V corroborates the results with case studies, and Section VI concludes the paper.

II. Problem Formulation

In this section, we present a framework of discrete optimal transport and then formulate an optimal transport problem with adversaries.

A. Discrete Optimal Transport

We denote $\mathscr{X} := \{1,...,|\mathscr{X}|\}$ the set of destinations (targets) that receive the resources, and $\mathscr{Y} := \{1,...,|\mathscr{Y}|\}$ the set of origins (sources) that distribute resources to the targets in a network. Each source node $y \in \mathscr{Y}$ is connected to a number of target nodes denoted by $\mathscr{X}_y$, representing that y can choose to allocate its resources to a specific group of destinations $\mathscr{X}_y$. Similarly, each target node $x \in \mathscr{X}$ can receive resources from multiple source nodes, and this set of resource suppliers to target x is denoted by $\mathscr{Y}_x$. Note that $\mathscr{X}_y$, $\forall y$ and $\mathscr{Y}_x$, $\forall x$ are nonempty. For convenience, we denote $\mathscr{E}$ as the set of all feasible transport paths in the network, i.e., $\mathscr{E} := \{\{x,y\} | x \in \mathscr{X}_y, y \in \mathscr{Y}_x\}$. Here, $\mathscr{E}$ also refers to the set of all edges in the established graph for resource transportation.

We next denote by $\pi_{xy} \in \mathbb{R}_+$ the amount of resources transported from the origin node $y \in \mathscr{Y}$ to the destination node $x \in \mathscr{X}$. We let $\Pi := \{\pi_{xy}\}_{x\in\mathscr{X},y\in\mathscr{Y}}$ be the designed transport plan. To this end, the centralized optimal transport problem can be formulated as follows:

$$\max_{\Pi} \sum_{x\in\mathscr{X}} \sum_{y\in\mathscr{Y}_x} t_{xy}(\pi_{xy}) + \sum_{y\in\mathscr{Y}} \sum_{x\in\mathscr{X}_y} s_{xy}(\pi_{xy}) \tag{1}$$

$$\text{s.t.} \quad \underline{p}_x \le \sum_{y\in\mathscr{Y}_x} \pi_{xy} \le \bar{p}_x, \ \forall x \in \mathscr{X}, \tag{1a}$$

$$\underline{q}_y \le \sum_{x\in\mathscr{X}_y} \pi_{xy} \le \bar{q}_y, \ \forall y \in \mathscr{Y}, \tag{1b}$$

$$\pi_{xy} \ge 0, \ \forall \{x,y\} \in \mathscr{E}, \tag{1c}$$

where $t_{xy} : \mathbb{R}_+ \to \mathbb{R}$ and $s_{xy} : \mathbb{R}_+ \to \mathbb{R}$ are utility functions for target node x and source node y, respectively. Furthermore, we set $\bar{p}_x \ge \underline{p}_x \ge 0$, $\forall x \in \mathscr{X}$ and $\bar{q}_y \ge \underline{q}_y \ge 0$, $\forall y \in \mathscr{Y}$. The constraints $\underline{p}_x \le \sum_{y\in\mathscr{Y}_x} \pi_{xy} \le \bar{p}_x$ and $\underline{q}_y \le \sum_{x\in\mathscr{X}_y} \pi_{xy} \le \bar{q}_y$ capture the limitations on the amount of requested and transferred resources at the target x and source y, respectively.

We have the following assumption on the utility functions.

Assumption 1. *The utility functions t_{xy} and s_{xy} are concave and monotonically increasing on π_{xy}, $\forall x \in \mathscr{X}, \forall y \in \mathscr{Y}$.*

Recall that a function f is concave on an interval if for any x and y in the interval and for any $\theta \in [0,1]$, $f((1-\theta)x + \theta y) \ge (1-\theta)f(x) + \theta f(y)$. A rich class of functions satisfy the conditions in Assumption 1. For example, t_{xy} and s_{xy} can be linear on π_{xy}, indicating a linear growth of benefits on the amount of transferred resources. These two functions can also admit a logarithmic form, capturing that the marginal utility decreases with the amount of transported resources.

B. Adversarial Optimal Transport

The attacker's goal is to minimize the aggregated transport utility by compromising the preference coefficients in the target's utility functions (which can happen at the information exchange stage). Specifically, the parameters in the utility function t_{xy} are compromised, for $x \in \mathscr{X}_a$, $y \in \mathscr{Y}_x$, where $\mathscr{X}_a$ denotes a subset of adversarial receiver nodes. Then, $\mathscr{X}_o := \mathscr{X} \setminus \mathscr{X}_a$ is the set of uncompromised targets. We denote by $\tilde{t}_{xy,\xi_{xy}}$ the modified utility under the attack, where ξ_{xy} represents the magnitude of the adversarial modifications on the corresponding parameters. For example, when the utility function admits a linear form as $t_{xy}(\pi_{xy}) = \delta_{xy}\pi_{xy}$, where $\delta_{xy} > 0$ is a parameter, the compromised utility form under the deception attack becomes $\tilde{t}_{xy,\xi_{xy}}(\pi_{xy}) = (\delta_{xy} + \xi_{xy})\pi_{xy}$. As another example, when t_{xy} takes a form of $t_{xy}(\pi_{xy}) = \delta_{xy}\min(\zeta_{xy}, \pi_{xy})$, where ζ_{xy} denotes a threshold after which the benefit of consuming more resources for target x from source y does not increase, the compromised utility form can be constructed as $\tilde{t}_{xy,\xi_{xy}}(\pi_{xy}) = (\delta_{xy} + \xi_{xy,1})\min\{\zeta_{xy} + \xi_{xy,2}, \pi_{xy}\}$. In this scenario, the attacker's action includes both $\xi_{xy,1}$ and $\xi_{xy,2}$, $\forall x \in \mathscr{X}_a$, $y \in \mathscr{Y}_x$. For a general scenario, we denote $\Xi := \{\xi_{xy}\}_{x\in\mathscr{X}_a, y\in\mathscr{Y}_x}$ as the attacker's deceptive strategy. Then, the adversarial optimal transport can be formulated as follows.

$$\begin{aligned} \max_{\Pi} \min_{\Xi} \ & \sum_{x\in\mathscr{X}_a} \sum_{y\in\mathscr{Y}_x} t_{xy}(\pi_{xy}) + \sum_{y\in\mathscr{Y}} \sum_{x\in\mathscr{X}_y} s_{xy}(\pi_{xy}) \\ & + \sum_{x\in\mathscr{X}_o} \sum_{y\in\mathscr{Y}_x} \tilde{t}_{xy,\xi_{xy}}(\pi_{xy}) + \sum_{x\in\mathscr{X}_a} \sum_{y\in\mathscr{Y}_x} l(\xi_{xy}) \\ \text{s.t.} \ & \text{(1a), (1b), (1c)}, \\ & \boldsymbol{\xi}_x \in \mathscr{A}_x, \ \forall x \in \mathscr{X}_a, \end{aligned} \tag{2}$$

where $\boldsymbol{\xi}_x := [\xi_{x1}, \xi_{x2}, ..., \xi_{x|\mathscr{Y}_x|}]$, for $x \in \mathscr{X}_a$; $\mathscr{A}_x$ is the attacker's feasible action set on the target node $x \in \mathscr{X}_a$; and $l : \mathbb{R} \to \mathbb{R}_+$ is a function capturing the cost of the attack.

Remark: The solution to the adversarial OT problem is related to the robust OT design. Robust OT also admits a minimax formulation but its goal is to find an optimal solution in the presence of structural and known uncertainties. Comparatively, in the adversarial OT, such uncertainty is replaced by strategic attacks, and the designed transport plan should be resistant to adversarial manipulations.

III. Adversarial Optimal Transport under Linear Utilities

In this section, we consider utility functions admitting a linear form for both the sender and receiver. Specifically, $t_{xy}(\pi_{xy}) = \delta_{xy}\pi_{xy}$ and $s_{xy}(\pi_{xy}) = \gamma_{xy}\pi_{xy}$, where $\delta_{xy}, \gamma_{xy} \in \mathbb{R}_+$. We assume that the attacker is capable to compromise a subset of target nodes in the network, denoted by $\mathscr{X}_a$. One interpretation is that the nodes in $\mathscr{X}_a$ do not have a secure communication protocol with the central planner. In comparison, the nodes in the set $\mathscr{X}_o = \mathscr{X} \setminus \mathscr{X}_a$ are able to set up high-confidence communication channels and hence are secure from adversarial attacks.

The attacker compromises the sensitive parameter δ_{xy}, $x \in \mathscr{X}_a, y \in \mathscr{Y}_x$, reported by the vulnerable target nodes and can modify them to new values aiming to decrease the social utility of resource transportation. The adversarial disruption can be regarded as a data poisoning attack, under which the utility parameter δ_{xy} is changed to $\tilde{\delta}_{xy} := \delta_{xy} + \xi_{xy}$. for $x \in \mathscr{X}_a, y \in \mathscr{Y}_x$. Here, ξ_{xy} denotes the action of the attacker, representing the magnitude of modification to the particular target utility parameter δ_{xy}. For convenience, we follow the notations in (2), where Ξ denotes the attacker's malicious manipulations on the utility parameters, and $\boldsymbol{\xi}_x$ is the attacker's action on the target node $x \in \mathscr{X}_a$.

To this end, the adversarial OT can be formulated in the following max-min format:

$$\begin{aligned} \max_{\Pi} \min_{\Xi} \; & U(\Pi, \Xi) = \sum_{x \in \mathscr{X}_o} \sum_{y \in \mathscr{Y}_x} \delta_{xy} \pi_{xy} + \sum_{y \in \mathscr{Y}} \sum_{x \in \mathscr{X}_y} \gamma_{xy} \pi_{xy} \\ & + \sum_{x \in \mathscr{X}_a} \sum_{y \in \mathscr{Y}_x} (\delta_{xy} + \xi_{xy}) \pi_{xy} + c_a \sum_{x \in \mathscr{X}_a} \|\boldsymbol{\xi}_x\|_1 \\ \text{s.t.} \quad & \text{(1a)}, \ \text{(1b)}, \ \text{(1c)}, \\ & \boldsymbol{\xi}_x \in \mathscr{A}_x, \ \forall x \in \mathscr{X}_a, \end{aligned} \tag{3}$$

where $c_a \in \mathbb{R}_+$ is a non-negative cost coefficient and $\mathscr{A}_x$ is the feasible action set of the attacker on target node x, $x \in \mathscr{X}_a$. U is the objective value under strategies Π and Ξ. The term $c_a \sum_{x \in \mathscr{X}_a} \|\boldsymbol{\xi}_x\|_1$ captures the cost of the attack. The sparsity induced by the l_1 norm is a convex approximation of the l_0 norm [9, Chapter 6] and indicates that the attacker has constraints on the number of compromise of utility parameters at a particular node $x \in \mathscr{X}_a$. The attacker is a minimizer of (3) as its goal is to minimize the aggregated transport utility reflected by the first three terms in the objective function U while using the least costly attack scheme captured by the last term in U.

Note that if the attacker modifies all the utility parameters significantly, it is easy for the planner to detect such adversarial perturbations. Also, the parameter $\tilde{\delta}_{xy}$ after compromise should still be non-negative. Thus, one form of $\mathscr{A}_x$ can be chosen as follows:

$$\mathscr{A}_x = \{\boldsymbol{\xi}_x | \|\boldsymbol{\xi}_x\|_2^2 \leq \kappa_x, \boldsymbol{\xi}_x + \boldsymbol{\delta}_x \geq \mathbf{0}\}, \ x \in \mathscr{X}_a, \tag{4}$$

where $\kappa_x \in \mathbb{R}_+$ denotes the upper limit of the standard norm of adversarial modifications at the target node $x \in \mathscr{X}_a$ by the attacker; $\boldsymbol{\delta}_x := [\delta_{x1}; \delta_{x2}; ...; \delta_{x|\mathscr{Y}_x|}]$; and $\mathbf{0}$ is a zero vector with appropriate dimension.

Problem (3) can be seen as a two-person zero-sum game denoted by G, where the transport planner is a maximizer and the attacker is a minimizer. The solution to the game G is characterized by the Nash equilibrium which predicts the outcome of the optimal transport strategy under adversarial environment. The formal definition of the Nash equilibrium strategy [5] is presented as follows.

Definition 1 (Nash Equilibrium)**.** *The strategy pair* $\{\Pi^*, \Xi^*\}$ *is a saddle-point Nash equilibrium of game G if*

$$U(\Pi, \Xi^*) \leq U(\Pi^*, \Xi^*) \leq U(\Pi^*, \Xi), \ \forall \ \Pi, \Xi, \tag{5}$$

where U is the objective function in (3)*.*

Solving game G requires addressing the formulated max-min problem (3). Specifically, both the central planner and the attacker need to compute their solutions holistically. This centralized computation paradigm does not scale well as the number of nodes in the transport network becomes large. Furthermore, to compute the solution Π, the central planner is required to have complete information on the transport network, including the utility parameters of all participants. Thus, it is imperative to design a computationally efficient mechanism to solve game G. Our subsequent goal is to solve problem (3) to obtain the equilibrium transport strategy by developing a distributed algorithm.

Note that the utility functions are not constrained to take a linear form. The developed analytical and computational results in the subsequent sections can be generalized to other scenarios for functions satisfying Assumption 1 straightforwardly such that the two-person game admits convex-concave property and min-max interchangeability.

IV. Analysis and Distributed Algorithm

In this section, we aim to design a fully distributed algorithm to compute the optimal strategies of the attacker and the participants by solving (3).

A. Equivalence between Max-Min and Minimax Problems

Before designing the algorithm, we prove that the formulated max-min problem (3) is equivalent to its minimax counterpart and hence show the existence of Nash equilibrium to game G. Specifically, we have the following results.

Proposition 1. *The max-min problem* (3) *yields the same solution as its minimax counterpart, i.e.,* $\min_{\Xi} \max_{\Pi} U(\Pi, \Xi)$ *subject to the same set of the constraints as in* (3)*. Thus, there exists a saddle point Nash equilibrium to game G. However, such equilibrium is not necessarily unique.*

Proof. The equivalence between max-min and minimax problems directly follows from the von Neumann's minimax theorem [10]. As the objective function U is not strictly concave in Π and not strictly convex in Ξ, the Nash equilibrium is not necessarily unique [5, Chapter 4]. ■

Note that Proposition 1 facilitates a convenient design of efficient mechanisms called best-response dynamics in finding the equilibrium strategies. We will design distributed update schemes for the attacker and the nodes in the subsequent Sections IV-B and IV-C, respectively, and then combine them together in Section IV-D.

B. Distributed Updates on the Deception Strategy

The attacker deceives the transport planner by compromising $\delta_{xy}, x \in \mathscr{X}_a, y \in \mathscr{Y}_x$, strategically. As the attacker's goal is to minimize U, a smaller $\tilde{\delta}_{xy}$ (hence a smaller δ_{xy}) will decrease the utility at the corresponding target node as indicated by the term $\sum_{x \in \mathscr{X}_a} \sum_{y \in \mathscr{Y}_x} (\delta_{xy} + \xi_{xy}) \pi_{xy}$. However, simply modifying the values of all δ_{xy}, $\forall x \in \mathscr{X}_a, y \in \mathscr{Y}_x$, to their minimum does not guarantee to minimize U. One reason is that the

transport strategy will change under attacks. Though the value of $\sum_{x\in\mathscr{X}_a}\sum_{y\in\mathscr{Y}_x}(\delta_{xy}+\xi_{xy})\pi_{xy}$ decreases, other terms such as $\sum_{x\in\mathscr{X}_o}\sum_{y\in\mathscr{Y}_x}\delta_{xy}\pi_{xy}$ and $\sum_{y\in\mathscr{Y}}\sum_{x\in\mathscr{X}_y}\gamma_{xy}\pi_{xy}$ may increase under the attack. Thus, the attacker's deceptive strategy is nontrivial to devise.

In the following, we describe how to leverage best-response dynamics to compute the strategy. Specifically, the attacker updates its decision Ξ by fixing the transport planner's strategy $\Pi'=\{\pi'_{xy}\}_{x\in\mathscr{X}_y,y\in\mathscr{Y}}$. In this regard, the first two terms in the objective function $U(\Pi,\Xi)$ and the first three constraints in (3) can be safely ignored as they are irrelevant with the attacker's deceptive strategy design. Thus, the attacker solves the following optimization program:

$$\begin{aligned}\min_{\Xi}\ &\sum_{x\in\mathscr{X}_a}\sum_{y\in\mathscr{Y}_x}\xi_{xy}\pi'_{xy}+c_a\sum_{x\in\mathscr{X}_a}\|\boldsymbol{\xi}_x\|_1\\ \text{s.t.}\ \ &\boldsymbol{\xi}_x\in\mathscr{A}_x,\ \forall x\in\mathscr{X}_a.\end{aligned}\tag{6}$$

The attacker can design the optimal deceptive strategy Ξ^* in a distributed fashion. First, we observe that the cost function in (6) is decoupled across vulnerable target nodes. Then, the optimal $\boldsymbol{\xi}^*_x$, $\forall x\in\mathscr{X}_a$, can be obtained separately. Solving (6) is thus equivalent to addressing $|\mathscr{X}_a|$ sub-problems as follows, for $x\in\mathscr{X}_a$,

$$\begin{aligned}\min_{\boldsymbol{\xi}_x}\ &\sum_{y\in\mathscr{Y}_x}\xi_{xy}\pi'_{xy}+c_a\|\boldsymbol{\xi}_x\|_1\\ \text{s.t.}\ \ &\boldsymbol{\xi}_x\in\mathscr{A}_x.\end{aligned}\tag{7}$$

We can further rewrite (7) in the following form, for $x\in\mathscr{X}_a$:

$$\begin{aligned}\min_{\boldsymbol{\xi}_x,\boldsymbol{\chi}_x}\ &\sum_{y\in\mathscr{Y}_x}\xi_{xy}\pi'_{xy}+\mathbf{1}^{\mathsf{T}}\boldsymbol{\chi}_x\\ \text{s.t.}\ \ &\boldsymbol{\xi}_x\in\mathscr{A}_x,\ c_a\boldsymbol{\xi}_x\le\boldsymbol{\chi}_x,\ c_a\boldsymbol{\xi}_x\ge-\boldsymbol{\chi}_x,\end{aligned}\tag{8}$$

where $\mathbf{1}$ is a vector of appropriate dimension with all ones; T denotes the transpose operator; and $\boldsymbol{\chi}_x$ is an auxiliary $|\mathscr{Y}_x|$-dimensional decision variable. Note that the objective function in (8) is linear and the constraints are convex, and thus (8) can be solved efficiently.

C. Distributed Updates on the Transport Strategy

Under the best-response mechanism, similarly, the transport planner determines the transport strategy by regarding the deceptive strategy $\Xi'=\{\xi'_{xy}\}_{x\in\mathscr{X}_a,y\in\mathscr{Y}_x}$ as fixed. Thus, the planner can omit the last term in the objective function $U(\Pi,\Xi)$ and the last constraint in (3) when making the decision. The planner's problem can be formulated as follows.

$$\begin{aligned}\max_{\Pi}\ &\sum_{x\in\mathscr{X}_o}\sum_{y\in\mathscr{Y}_x}\delta_{xy}\pi_{xy}+\sum_{y\in\mathscr{Y}}\sum_{x\in\mathscr{X}_y}\gamma_{xy}\pi_{xy}\\ &+\sum_{x\in\mathscr{X}_a}\sum_{y\in\mathscr{Y}_x}(\delta_{xy}+\xi'_{xy})\pi_{xy}\\ \text{s.t.}\ \ &\text{(1a), (1b), (1c).}\end{aligned}\tag{9}$$

Solving (9) in a centralized manner requires the transport planner to know all parameters including δ_{xy} and γ_{xy}, $\forall\{x,y\}\in\mathscr{E}$. Our next goal is to design a distributed method to compute the optimal Π in (9). First, we introduce auxiliary variables π^t_{xy} and π^s_{xy} denoting the amount of resources requested by target x from source y and source y offering to target x, respectively. These two transport plans should be equal to each other to reach a consensus. Thus, we have constraints $\pi^t_{xy}=\pi_{xy}$ and $\pi_{xy}=\pi^s_{xy}$, $\forall\{x,y\}\in\mathscr{E}$. Then, (9) can be reformulated as

$$\begin{aligned}\min_{\Pi^t\in\mathscr{F}_t,\Pi^s\in\mathscr{F}_s,\Pi}\ &-\sum_{x\in\mathscr{X}_o}\sum_{y\in\mathscr{Y}_x}\delta_{xy}\pi^t_{xy}-\sum_{y\in\mathscr{Y}}\sum_{x\in\mathscr{X}_y}\gamma_{xy}\pi^s_{xy}\\ &-\sum_{x\in\mathscr{X}_a}\sum_{y\in\mathscr{Y}_x}(\delta_{xy}+\xi'_{xy})\pi^t_{xy}\\ \text{s.t.}\ \ &\pi^t_{xy}=\pi_{xy},\forall\{x,y\}\in\mathscr{E},\\ &\pi_{xy}=\pi^s_{xy},\forall\{x,y\}\in\mathscr{E},\end{aligned}\tag{10}$$

where $\Pi^t:=\{\pi^t_{xy}\}_{x\in\mathscr{X}_y,y\in\mathscr{Y}}$, $\Pi^s:=\{\pi^s_{xy}\}_{x\in\mathscr{X},y\in\mathscr{Y}_x}$, $\mathscr{F}_t:=\{\Pi^t|\pi^t_{xy}\ge0,\underline{p}_x\le\sum_{y\in\mathscr{Y}_x}\pi^t_{xy}\le\bar{p}_x,\{x,y\}\in\mathscr{E}\}$, and $\mathscr{F}_s:=\{\Pi^s|\pi^s_{xy}\ge0,\underline{q}_y\le\sum_{x\in\mathscr{X}_y}\pi^s_{xy}\le\bar{q}_y,\{x,y\}\in\mathscr{E}\}$.

From the convex form of the formulation we can obtain the Lagrangian:

$$\begin{aligned}L(\Pi_t,\Pi_s,\Pi,\alpha^t_{xy},\alpha^s_{xy})=&-\sum_{x\in\mathscr{X}_o}\sum_{y\in\mathscr{Y}_x}\delta_{xy}\pi^t_{xy}-\sum_{y\in\mathscr{Y}}\sum_{x\in\mathscr{X}_y}\gamma_{xy}\pi^s_{xy}\\ &-\sum_{x\in\mathscr{X}_a}\sum_{y\in\mathscr{Y}_x}\left(\delta_{xy}+\xi'_{xy}\right)\pi^t_{xy}+\sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}_x}\alpha^t_{xy}\left(\pi^t_{xy}-\pi_{xy}\right)\\ &+\sum_{y\in\mathscr{Y}}\sum_{x\in\mathscr{X}_y}\alpha^s_{xy}\left(\pi_{xy}-\pi^s_{xy}\right)+\frac{\eta}{2}\sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}_x}\left(\pi^t_{xy}-\pi_{xy}\right)^2\\ &+\frac{\eta}{2}\sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}_x}\left(\pi_{xy}-\pi^s_{xy}\right)^2.\end{aligned}\tag{11}$$

Here, α^t_{xy} and α^s_{xy} are Lagrangian multipliers associated with the constraints, and η is a positive constant.

Theorem 1. *We obtain the following steps by applying ADMM algorithm to* (11)*:*

$$\begin{aligned}\Pi^t_x(k+1)\in\arg\min_{\Pi^t_x\in\mathscr{F}^t_x}&-\sum_{y\in\mathscr{Y}_x}\delta_{xy}\pi^t_{xy}+\sum_{y\in\mathscr{Y}_x}\alpha^t_{xy}(k)\pi^t_{xy}\\ &+\frac{\eta}{2}\sum_{y\in\mathscr{Y}_x}\left(\pi^t_{xy}-\pi_{xy}(k)\right)^2,\ \text{for } x\in\mathscr{X}_o,\end{aligned}\tag{12}$$

$$\begin{aligned}\Pi^t_x(k+1)\in\arg\min_{\Pi^t_x\in\mathscr{F}^t_x}&-\sum_{y\in\mathscr{Y}_x}\left(\delta_{xy}+\xi'_{xy}\right)\pi^t_{xy}\\ &+\sum_{y\in\mathscr{Y}_x}\alpha^t_{xy}(k)\pi^t_{xy}+\frac{\eta}{2}\sum_{y\in\mathscr{Y}_x}\left(\pi^t_{xy}-\pi_{xy}(k)\right)^2,\ \text{for } x\in\mathscr{X}_a,\end{aligned}\tag{13}$$

$$\begin{aligned}\Pi^s_y(k+1)\in\arg\min_{\Pi^s_y\in\mathscr{F}^s_y}&-\sum_{x\in\mathscr{X}_y}\gamma_{xy}\pi^s_{xy}+\sum_{x\in\mathscr{X}_y}\alpha^s_{xy}(k)\pi^s_{xy}\\ &+\frac{\eta}{2}\sum_{x\in\mathscr{X}_y}\left(\pi_{xy}(k)-\pi^s_{xy}\right),\end{aligned}\tag{14}$$

$$\begin{aligned}\pi_{xy}(k+1)\in\arg\min_{\pi_{xy}}&\,\alpha^t_{xy}(k)\pi_{xy}+\alpha^s_{xy}(k)\pi_{xy}\\ &+\frac{\eta}{2}(\pi^t_{xy}(k+1)-\pi_{xy})^2+\frac{\eta}{2}(\pi_{xy}-\pi^s_{xy}(k+1))^2,\end{aligned}\tag{15}$$

$$\alpha^t_{xy}(k+1)=\alpha^t_{xy}(k)+\eta(\pi^t_{xy}(k+1)-\pi_{xy}(k+1))^2,\tag{16}$$

$$\alpha^s_{xy}(k+1)=\alpha^s_{xy}(k)+\eta(\pi_{xy}(k+1)-\pi^s_{xy}(k+1))^2,\tag{17}$$

where $\Pi^t_{\tilde{x}}=\{\pi^t_{xy}\}_{y\in\mathscr{Y}_x,x=\tilde{x}}$ *and* $\Pi^s_{\tilde{y}}=\{\pi^s_{xy}\}_{x\in\mathscr{X}_y,y=\tilde{y}}$ *denote the transport strategy computed by target node* $\tilde{x}$ *and source node* $\tilde{y}$*, respectively.*

Additionally, we define $\mathscr{F}^t_x:=\{\Pi^t_x|\pi^t_{xy}\ge0,y\in\mathscr{Y}_x,\underline{p}_x\le\sum_{y\in\mathscr{Y}_x}\pi^t_{xy}\le\bar{p}_x\}$ *and* $\mathscr{F}^s_y:=\{\Pi^s_y|\pi^s_{xy}\ge0,x\in\mathscr{X}_y,\underline{q}_y\le\sum_{x\in\mathscr{X}_y}\pi^s_{xy}\le\bar{q}_x\}$.

Proof. Let $\vec{x} = [\vec{\Pi}_x^{t\mathsf{T}}, \vec{\Pi}^{\mathsf{T}}]^{\mathsf{T}}$, $\vec{y} = [\vec{\Pi}^{\mathsf{T}}, \vec{\Pi}_y^{s\mathsf{T}}]^{\mathsf{T}}$, and $\alpha = [\{\alpha_{xy}^s\}^{\mathsf{T}}, \{\alpha_{xy}^t\}^{\mathsf{T}}]^{\mathsf{T}}$, where T and $\vec{\cdot}$ denote the transpose and vectorization operator. Note that these three vectors are all $2|\mathscr{E}| \times 1$. Now we can write the constraints in (10) in a matrix form such that $\mathbf{A}\vec{x} = \vec{y}$, where $\mathbf{A} = [\mathbf{I}, \mathbf{0}; \mathbf{0}, \mathbf{I}]$ with $\mathbf{I}$ and $\mathbf{0}$ denoting the $|\mathscr{E}|$-dimensional identity and zero matrices, respectively. Next, we note that $\vec{x} \in \mathscr{F}_{\vec{x}}^t$ and $\vec{y} \in \mathscr{F}_{\vec{y}}^s$, where $\mathscr{F}_{\vec{x}}^t = \{\vec{x} | \pi_{xy}^t \geq 0, \underline{p}_x \leq \sum_{y \in \mathscr{Y}_x} \pi_{xy}^t \leq \bar{p}_x, \{x,y\} \in \mathscr{E}\}$, $\mathscr{F}_{\vec{y}}^s := \{\vec{y} | \pi_{xy}^s \geq 0, \underline{q}_y \leq \sum_{x \in \mathscr{X}_y} \pi_{xy}^s \leq \bar{q}_y, \{x,y\} \in \mathscr{E}\}$. Then, we can solve (10) using the iterations: 1) $\vec{x}(k+1) \in \arg\min_{\vec{x} \in \mathscr{F}_{\vec{x}}^t} L(\vec{x}, \vec{y}(k), \alpha(k))$; 2) $\vec{y}(k+1) \in \arg\min_{\vec{y} \in \mathscr{F}_{\vec{y}}^s} L(\vec{x}(k+1), \vec{y}, \alpha(k))$; 3) $\alpha(k+1) = \alpha(k) + \eta(A\vec{x}(k+1) - \vec{y}(k+1))$, based on [9]. Because we have no couplings among $\Pi_x^t, \Pi_y^s, \Pi, \alpha_{xy}^t$ and α_{xy}^s, the above iterations can be equivalently decomposed to (12)-(17). ■

Proposition 2. *Iterations* (15)-(17) *can be simplified as:*

$$\pi_{xy}(k+1) = \frac{1}{2}\left(\pi_{xy}^t(k+1) + \pi_{xy}^s(k+1)\right), \tag{18}$$

$$\alpha_{xy}(k+1) = \alpha_{xy}(k) + \frac{\eta}{2}\left(\pi_{xy}^t(k+1) - \pi_{xy}^s(k+1)\right). \tag{19}$$

Proof. As (15) is strictly concave, we can solve it by first-order condition: $\pi_{xy}(k+1) = \frac{1}{2\eta}(\alpha_{xy}^t(k) - \alpha_{xy}^s(k)) + \frac{1}{2}(\pi_{xy}^t(k+1) + \pi_{xy}^s(k+1))$. By substituting the above equation into (16) and (17), we get $\alpha_{xy}^t(k+1) = \frac{1}{2}(\alpha_{xy}^t(k) + \alpha_{xy}^s(k)) + \frac{\eta}{2}(\pi_{xy}^t(k+1) - \pi_{xy}^s(k+1))$, $\alpha_{xy}^s(k+1) = \frac{1}{2}(\alpha_{xy}^t(k) + \alpha_{xy}^s(k)) + \frac{\eta}{2}(\pi_{xy}^t(k+1) - \pi_{xy}^s(k+1))$. Thus, $\alpha_{xy}^t = \alpha_{xy}^s$ during each update. Then, $\pi_{xy}(k+1)$ can be simplified as $\pi_{xy}(k+1) = \frac{1}{2}(\pi_{xy}^t(k+1) + \pi_{xy}^s(k+1))$ shown in (18). In addition, we can achieve (16) and (17) from $\alpha_{xy}^t = \alpha_{xy}^s = \alpha_{xy}$ in (19). ■

Theorem 2. *The algorithm in Theorem 1 with simplifications in Proposition 2 converges to an optimal solution.*

Proof. The convergence of the algorithm directly follows from the general arguments in [9, Section 3.2]. ■

In the above proposed distributed algorithm, each node computes its transport strategy based on the local information, i.e., information of connected nodes rather than all the nodes. The nodes update their strategies iteratively by communicating with connected neighbors. This is different from the centralized computation where the central planner needs to know all nodes' information to design the transport plan and then broadcasts the decision to the nodes.

D. Integrated Distributed Algorithm

We combine the algorithms for the attacker and the participants into one distributed algorithm. The integrated algorithm follows the updates below.

$$\begin{aligned} \boldsymbol{\xi}_x(k+1) \in \arg\min_{\boldsymbol{\xi}_x, \boldsymbol{\chi}_x} & \sum_{y \in \mathscr{Y}_x} \xi_{xy}\pi_{xy}(k) + \mathbf{1}^{\mathsf{T}}\boldsymbol{\chi}_x \\ \text{s.t.} \quad & \boldsymbol{\xi}_x \in \mathscr{A}_x,\ c_a\boldsymbol{\xi}_x \leq \boldsymbol{\chi}_x,\ c_a\boldsymbol{\xi}_x \geq -\boldsymbol{\chi}_x. \end{aligned} \tag{20}$$

$$\begin{aligned} \Pi_x^t(k+1) \in \arg\min_{\Pi_x^t \in \mathscr{F}_x^t} & -\sum_{y \in \mathscr{Y}_x} \delta_{xy}\pi_{xy}^t + \sum_{y \in \mathscr{Y}_x} \alpha_{xy}(k)\pi_{xy}^t \\ & + \frac{\eta}{2}\sum_{y \in \mathscr{Y}_x}\left(\pi_{xy}^t - \pi_{xy}(k)\right)^2, \text{ for } x \in \mathscr{X}_o, \end{aligned} \tag{21}$$

$$\begin{aligned} \Pi_x^t(k+1) \in \arg\min_{\Pi_x^t \in \mathscr{F}_x^t} & -\sum_{y \in \mathscr{Y}_x} (\delta_{xy} + \xi_{xy}(k))\,\pi_{xy}^t \\ & + \sum_{y \in \mathscr{Y}_x} \alpha_{xy}(k)\pi_{xy}^t + \frac{\eta}{2}\sum_{y \in \mathscr{Y}_x}\left(\pi_{xy}^t - \pi_{xy}(k)\right)^2, \text{ for } x \in \mathscr{X}_a, \end{aligned} \tag{22}$$

$$\begin{aligned} \Pi_y^s(k+1) \in \arg\min_{\Pi_y^s \in \mathscr{F}_y^s} & -\sum_{x \in \mathscr{X}_y} \gamma_{xy}\pi_{xy}^s + \sum_{x \in \mathscr{X}_y} \alpha_{xy}(k)\pi_{xy}^s \\ & + \frac{\eta}{2}\sum_{x \in \mathscr{X}_y}\left(\pi_{xy}(k) - \pi_{xy}^s\right), \end{aligned} \tag{23}$$

$$\pi_{xy}(k+1) = \frac{1}{2}\left(\pi_x^t(k+1) + \pi_y^s(k+1)\right), \tag{24}$$

$$\alpha_{xy}(k+1) = \alpha_{xy}(k) + \frac{\eta}{2}\left(\pi_{xy}^t(k+1) - \pi_{xy}^s(k+1)\right). \tag{25}$$

The convergence of the integrated distributed algorithm is worth investigation. We have the following result.

Theorem 3. *The designed integrated distributed algorithm* (20)-(25) *converges to a saddle-point equilibrium.*

Proof. Based on Proposition 1, we know that there exists an equilibrium with $\{\boldsymbol{\xi}_x^*\}_{x \in \mathscr{X}_a}$ and Π^* to the minimax game G. Theorem 2 further shows that the max-problem (9) converges to the best response of the min-problem (8). Note that the trajectory of best response dynamics for continuous concave-convex zero-sum games always converges to saddle points [11]. Thus, the developed integrated distributed algorithm (20)-(25) converges to $\{\boldsymbol{\xi}_x^*\}_{x \in \mathscr{X}_a}$ and Π^*. ■

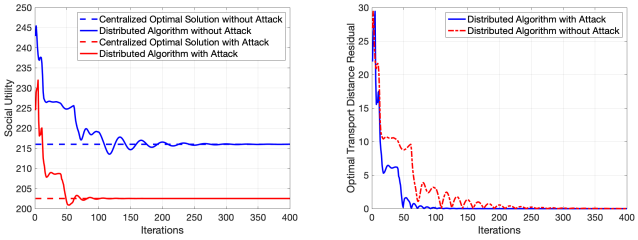
For convenience, we summarize the integrated distributed algorithm in Algorithm 1.

Algorithm 1 Integrated Distributed Algorithm

1: **while** $\boldsymbol{\xi}_x$, Π_x^t and Π_y^s not converging **do**
2: Compute $\boldsymbol{\xi}_x(k+1)$ using (20), $\forall x \in \mathscr{X}_a$
3: Compute $\Pi_x^t(k+1)$ using (21), $\forall x \in \mathscr{X}_o$
4: Compute $\Pi_x^t(k+1)$ using (22), $\forall x \in \mathscr{X}_a$
5: Compute $\Pi_y^s(k+1)$ using (23), $\forall y \in \mathscr{Y}$
6: Compute $\pi_{xy}(k+1)$ using (24), $\forall \{x,y\} \in \mathscr{E}$
7: Compute $\alpha_{xy}(k+1)$ using (25), $\forall \{x,y\} \in \mathscr{E}$
8: **end while**
9: **return** $\boldsymbol{\xi}_x(k+1)$, $\forall x \in \mathscr{X}_a$ and $\pi_{xy}(k+1)$, $\forall \{x,y\} \in \mathscr{E}$

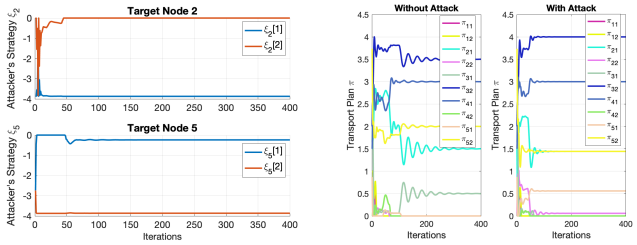
V. Case Studies

In this section we corroborate our algorithm for distributed OT while considering adversarial opponents. We consider the first case with five target nodes and two source nodes with a network structure connecting every source node to every target node. The upper bounds for the source nodes are $\bar{p}_1 = 2$, $\bar{p}_2 = 3$, $\bar{p}_3 = 4$, $\bar{p}_4 = 3$, $\bar{p}_5 = 2$, $\bar{q}_1 = 5$, and $\bar{q}_2 = 5.5$. The lower bound for all nodes are set to 0. Additionally, we consider linear utility functions $t_{xy}(\pi_{xy}) = \delta_{xy}\pi_{xy}$, and $s_{xy}(\pi_{xy}) = \gamma_{xy}\pi_{xy}, \forall \{x,y\} \in \mathscr{E}$. The corresponding parameters in the linear functions are selected as follows: $[\delta_{xy}]_{x \in \mathscr{X}, y \in \mathscr{Y}} = \begin{bmatrix} 4 & 12 & 4 & 12 & 8 \\ 8 & 8 & 16 & 4 & 4 \end{bmatrix}$, $[\gamma_{xy}]_{x \in \mathscr{X}, y \in \mathscr{Y}} = \begin{bmatrix} 6 & 4.5 & 12 & 6 & 9 \\ 3 & 6 & 7.5 & 9 & 12 \end{bmatrix}$. The adversary's parameters are $c_a =$



(a) Social Utility (b) Distance Residual

Fig. 1: Impact of the adversarial attacks on the transport strategy design. (a) and (b) depict the trajectories of social utility and residual of transport strategy, respectively.



(a) Attacker's Strategy (b) Transport Plan

Fig. 2: (a) shows the attacker's strategy at the target nodes 2 and 5. (b) shows the corresponding transport plans.

0.5 and $\kappa_x = 15$, $\forall x \in \mathcal{X}_a$, and the deceptive targets include nodes 2 and 5. We next design the resilient transport strategy using the proposed distributed algorithm.

First, we show that the algorithm works and converges to the same value obtained by the centralized method. We also compare the transport strategies when the network with and without adversaries. When there is an adversary, we use a combination of (21) (for benign targets) and (22) (for deceptive targets) to calculate $\Pi_x^t(k+1)$. When there is no adversary, meaning none of the nodes are compromised, we only use (22) to compute Π_x^t. The results are shown in Fig. 1. Specifically, Fig. 1(a) shows the social utility which is the aggregated payoff of all nodes. Fig. 1(a) highlights that the algorithm converges to the centralized solution in both scenarios with and without attacks. We also note that when we consider an attack the algorithm converges to a lower social utility. This is due to the fact that we have to account for the adversarial impacts which decreases the desired utility between the source node and the compromised target node. Fig. 1(b) highlights the distance residual of the transport strategy, which measures the difference between the strategy at each step and the equilibrium solution. The attacker's strategy $\boldsymbol{\xi}_x$ is shown in Fig. 2(a). For both compromised nodes, the deceptive strategies $\boldsymbol{\xi}_2$ and $\boldsymbol{\xi}_5$ converge to a nonzero values, indicating that the attacker is actively affecting the transport plan. Fig. 2(b) further illustrates this phenomenon as the resource allocation strategies are different in the two investigated cases.

We further investigate a larger scale network with 30 targets and 3 sources. The results can be found in [12].

VI. Conclusion

In this paper, we have investigated an adversarial discrete optimal transport framework for resource matching in which the participating nodes could be malicious by reporting untruthful preference parameters. We have developed a distributed algorithm for computing the strategic resource allocation strategies which are resilient to such attacks. The designed algorithm converges to a same solution as one designed by a centralized planner, and it is applicable to large scale networks susceptible to deceptive attacks. The adversarial behavior is specifically acknowledged in the algorithm when a participating node is compromised. Each connected pair of target and source nodes negotiate on the their proposed transport plans, and thus the compromised node's actions is taken into account in the final allocation schemes. The algorithm terminates when the sources and targets reach a consensus. Future work includes to consider the differential privacy of the nodes when designing the algorithm. Another direction is to develop a formal metric to quantify the stealthiness of the attacker and integrate it with the established adversarial optimal transport framework.

References

[1] A. Galichon, *Optimal Transport Methods in Economics*. Princeton University Press, 2016.

[2] S. Bayat, Y. Li, L. Song, and Z. Han, "Matching theory: Applications in wireless communications," *IEEE Signal Processing Magazine*, vol. 33, no. 6, pp. 103–122, 2016.

[3] R. Zhang and Q. Zhu, "Consensus-based distributed discrete optimal transport for decentralized resource matching," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 5, no. 3, pp. 511–524, 2019.

[4] J. Hughes and J. Chen, "Fair and distributed dynamic optimal transport for resource allocation over networks," in *55th Annual Conference on Information Sciences and Systems (CISS)*, 2021.

[5] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*. SIAM, 1998.

[6] A. Garnaev and W. Trappe, "Fair resource allocation under an unknown jamming attack: a bayesian game," in *IEEE International Workshop on Information Forensics and Security (WIFS)*, 2014, pp. 227–232.

[7] G. Shao, R. Wang, X.-F. Wang, and K.-Z. Liu, "Distributed algorithm for resource allocation problems under persistent attacks," *Journal of the Franklin Institute*, vol. 357, no. 10, pp. 6241–6256, 2020.

[8] H. Chen, M. Zhou, L. Xie, K. Wang, and J. Li, "Joint spectrum sensing and resource allocation scheme in cognitive radio networks with spectrum sensing data falsification attack," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 11, pp. 9181–9191, 2016.

[9] S. Boyd, N. Parikh, and E. Chu, *Distributed Optimization and Statistical Learning via the Alternating Direction Method of Multipliers*. Now Publishers, 2011.

[10] H. Nikaidô, "On von Neumann's minimax theorem," *Pacific Journal of Mathematics*, vol. 4, no. 1, pp. 65–72, 1954.

[11] J. Hofbauer and S. Sorin, "Best response dynamics for continuous zero–sum games," *Discrete & Continuous Dynamical Systems-B*, vol. 6, no. 1, p. 215, 2006.

[12] J. Hughes and J. Chen, "Resilient and distributed discrete optimal transport with deceptive adversary: A game-theoretic approach," https://arxiv.org/abs/2106.07455, 2021, [Online].