University Library



A gateway to Melbourne's research publications

Minerva Access is the Institutional Repository of The University of Melbourne

Author/s:
Chorppath, AK;Alpcan, T;Boche, H

Title:
Adversarial Behavior in Network Games

Date:
2015-03-01

Citation:
Chorppath, A. K., Alpcan, T. & Boche, H. (2015). Adversarial Behavior in Network Games. DYNAMIC GAMES AND APPLICATIONS, 5 (1), pp.26-64. https://doi.org/10.1007/s13235-014-0120-4.

Persistent Link:
https://hdl.handle.net/11343/241546

Adversarial Behavior in Network Games

Anil Kumar Chorppath
Technical University of Munich
Munich, Germany
Email: anil.chorppath@tum.de

Tansu Alpcan
The University of Melbourne
Melbourne, Australia
Email: tansu.alpcan@unimelb.edu.au

Holger Boche
Technical University of Munich
Munich, Germany
Email: boche@tum.de

Abstract

This paper studies the effects of and countermeasures against adversarial behavior in network resource allocation mechanisms such as pricing and auctions. It models the heterogeneous behavior of users, which ranges from altruistic to selfish and to malicious, using game theory. The paper adopts a mechanism design approach to quantify the effect of adversarial behavior and modify the mechanisms to respond. First, the *Price of Malice* of the existing network mechanisms to adversarial behavior, which ranges from extreme selfishness to destructive maliciousness, is analyzed. An iterative distributed pricing algorithm is proposed and its dynamics and convergence properties are analyzed. The resistance of the presented mechanism collusions, which constitute another kind of malicious behavior, is investigated. Next, the assumption that the malicious user has information about the utility function of selfish users is relaxed and a regression-based iterative learning scheme for the malicious user is presented and applied to both pricing and auction mechanisms. Differentiated pricing as method to counter such adversarial behaviors is then briefly discussed. The results obtained are illustrated with multiple examples and numerical simulations.

Keywords: Adversarial behavior, mechanism design, game theory, dynamic games, detection and counter measures, interference management, regression learning, rate control.

I. Introduction

The behavior of different users (players) on networks may range from altruistic on the one end to malicious (adversarial) on the other end of a wide spectrum. While altruistic users aim to improve the overall network performance, a selfish player strategies to maximize her throughput by getting the proportional share of resources. A malicious user, however, tries to get a disproportionate share of network resource, and in addition may disrupt the whole network. Well-known examples of this adversarial behavior in networks include jamming in wireless networks and denial-of-service (DoS) attacks [1]- [2].

In this paper, we model the coexistence of altruistic, selfish and malicious players using a noncooperative game theoretic formulation [3]. We adopt a mechanism design [4] approach in which a designer designs rules and incentives to control the outcome of the underlying game between the players. The designer try to achieve some desirable properties for the mechanism whose definitions are given in the appendix attached to the end of the paper. We study the the effect of altruistic and malicious players in the games and mechanisms where the players are usually modeled as selfish. Here, we assume that malicious users mainly stay within the rules of of the system but exhibit adversarial behavior. We model them by assigning different utility functions than selfish players, such as own selfish utility minus the sum of utility of other users in the system or a convex one in contrast to the usually concave utility functions of selfish users. Thus, we map their destructive behavior such as jamming other players and launching Denial-of-Service(DoS) attacks to rational incentives.

The classical Vicrey-Clarke-Groves(VCG) mechanism [5] is efficient and truth revealing in the presence of selfish players. We first show the effect of the adversarial behavior of some users in the efficiency of VCG mechanism to motivate the need to quantify the effect of the adversarial behavior in network mechanisms.

To analyze the effects of adversarial behavior, we quantify the robustness of some known network mechanisms with respect to the adversarial behavior of (some of) their participants. A modified version the metric called Price of Malice [6]- [7] is defined suitable for games in network resource allocation and applied to two different network problems dealt here. In the cases analyzed, the malicious players are assumed to take the maximum resource share possible without detection and that way try to disrupt others.

Another behavior which is adversarial and specific to the context of mechanisms is that some of the malicious users form a group or *collusion* and destroy some of the mechanisms desirable properties. The mechanisms which are resistant to collusion are called group strategy-proof mechanisms. In Section VI-A, we investigate the group strategy-proof property of one of the mechanisms proposed for network resource sharing setting and analyze the effect of adversarial behavior resulting from collusion.

This work has been supported in part by Deutsche Telekom Laboratories, Berlin, Germany. A conference version of this work has appeared in proceedings of Gamecomm 2011, May 2011, Cachen, France.

Since it is not realistic to assume that the malicious user have complete knowledge of the utility function of the selfish users learning techniques can be used by the malicious user to infer this information. Gaussian regression learning is used for marginal utility function estimation by the malicious user using which it can calculate its best response. Learning is a good tool for the malicious user to estimate the behavior of other users and manipulate the mechanisms accordingly. We consider the scenario where regression learning techniques are used by the malicious user to learn the utility functions of the regular users. Both pricing and auction mechanisms are considered for this case. In [8], Gaussian regression learning techniques are used in the general context of mechanism design. In this paper, we use Gaussian regression learning method [9] to learn the utilities by the malicious user by observing the actions of the regular users.

To counter the adversarial behavior, we design mechanisms in which the prices are varied differentially to punish the malicious players after detecting them using any threshold detection technique based on the bids of users. Clearly, when the malicious users does not abide by the rules and vandalize the system, harder responses such as blocking the malicious users after detection are required. We employ a differentiated pricing scheme in which both aggressively selfish and malicious players with disproportional usage of resources are made to pay higher prices than regular selfish players. The vulnerability of this method is quantified using a specific trade-off metric defined.

We consider two different types of network problems in this paper, which differ in coupling of users, i.e. how their actions affect each other, and resource sharing methods. The first one is rate (congestion) control with additive resource sharing, e.g. sharing of bandwidth at a link with fixed capacity. The second one is interference management, e.g. uplink power control in CDMA wireless networks with interference coupling. While allocating these divisible resources to selfish users, a loss in social welfare is caused at the resulting Nash equilibrium due to the selfish nature often referred as Price of Anarchy. Mechanisms such as auctions and pricing mechanisms are proposed to shift the Nash equilibrium point to efficient point. In these mechanisms and underlying games, the selfish nature of rational users were modeled with concave utility functions. But in practical situations, there are altruistic users who care for the welfare of all the users and adversarial users who may deviate from equilibrium point even if it causes loss to them or will show extreme selfishness, i.e. they behave 'irrationally' if modeled using this class of utility functions. We retain the rationality assumption by associating them with different utility functions. In the presence of the these altruistic and adversarial agents, the mechanisms employed will have Nash equilibrium different from the efficient point and this deviation is captured in the metric Price of Malice. In this paper, Price of Malice is quantified for some specific network mechanisms and these mechanisms are modified to punish the adversarial users to make them come back to regular selfish behavior, which brings the system to the efficient Nash equilibrium point.

The main contributions of this paper include:

1) Showing the effect of malicious behavior in VCG Mechanism.
2) Quantifying the Price of Malice and related metrics in various network mechanisms with adversarial users.
3) The convergence proof of the iterative distributed algorithm for the pricing mechanism.
4) Analyzing the resistance of mechanisms against coalitions of malicious players, i.e. whether it is group strategy-proof or not.
5) Quantifying the Price of Collusion in network mechanisms.
6) Design of differentiated pricing scheme to punish adversarial users and definition of a trade-off parameter.
7) Analysis of learning the utility function of selfish users by malicious users.

A. Related works

In networked systems with selfish users, a loss in overall social welfare was identified and referred as *Price of Anarchy* [10], [11]. In the presence of malicious users this concept was extended and *Price of Byzantine Anarchy* and *Price of Malice* was first introduced in [6]. They obtained bounds on these metrics which are parameterized by the number of malicious users for a virus inoculation game for social networks. A modified definition was proposed in [7] for congestion games based on the delay experienced at Nash equilibrium point with and without the presence of a malicious player. Both of these works have observed a *Windfall of Malice*, where malicious behavior actually improves the social welfare of non-oblivious selfish users due to the better cooperation resulting because of the 'fear factor' or effects similar to Braess's paradox [7]. In [12] a more general definition of Price of Malice is given with weaker assumptions than above mentioned works in the presence of Byzantine players and using a no-regret analysis. A game theoretic model for the strategic interaction of legitimate and malicious players is introduced in [13], where the authors have derived a bound on the damage caused by the malicious players. In [14], partial altruism of some of the users is analyzed and a bound on Price of Anarchy was obtained as a function of the altruism parameter. To get around with *Price of Anarchy*, pricing for price taking users [15]–[17] and auctions for price anticipating users [18], [19] are employed. In [20], the effect of spiteful behavior of some of the users is analyzed in the context of first and second price auctions and the revenue obtained is compared. In [21], the Degree of Cooperation of a user as a vector of values which are used to obtain a convex combination of utility of other users to model altruistic behavior is introduced in the context of routing games in a network. The Value of Unilateral Altruism (VoU) is defined to be the ratio of the equilibrium utility of the altruistic user to the equilibrium utility she would have received in Nash equilibrium if she was selfish and is calculated

for routing games in [22]. In this paper, we quantify the Price of Malice of the mechanisms proposed for network resource allocation and modify the rules of these mechanisms to counter the malicious behavior.

There are works in mechanism design literature, e.g. [23], [24], addressing the issue of some (malicious) players forming a coalition and gaining unfair advantage by misleading the designer. Such *collusion* behavior is adversarial to the mechanism because it destroys some of its desirable properties. These works have developed group-strategy proof mechanisms which are resistant to collusion. Price of Collusion was introduced in [25] as the worst possible ratio between the social cost at equilibrium before and after the collusion scenario. Some other metrics to quantify the effect of collusion were defined in [26] and obtained in the context of load balancing games.

There has been a lot of work on games and mechanisms with incomplete information. Games with Bayesian players been studied a lot in works starting with [27]. Subjectivity and Correlated equilibria were also studied in the context of incomplete information [28]. In [29], the authors reduce mechanism design problems to standard algorithmic problems using techniques from sample complexity. In [8], Gaussian regression learning is used to estimate the marginal utilities of the users in a network mechanism design setting by the designer. We follow the learning approach where malicious user learns the selfish user utility functions.

To counter the adversarial behavior, Micali & Valiant in [30], have developed a modified Vickrey-Clarke-Groves(VCG) mechanism, taking into account collusive, irrational, and adversarial behavior for combinatorial auctions. In the proposed mechanism, the price charged to an agent is increased from VCG price by a scaled factor of the maximum social welfare of other agents. In spirit of this, we also modify the pricing in the proportional fair allocation mechanisms to punish the malicious users and incentivise them to come to regular selfish behavior.

The rest of the paper is organized as follows. The next section presents the underlying mechanism design model. Subsequently, Section IV quantifies the Price of Malice of the network mechanisms with respect to the adversarial behavior. Section VI-A investigates the effect of collusive adversarial behavior in a mechanism and checks for its group strategy-proof property. Then in Section VII, the case where regression learning techniques are used by the malicious user to learn the utilities of regular users is discussed. In Section VIII, a differentiated pricing scheme to counter the adversarial behavior is introduced and a method to detect malicious agents is presented. Numerical simulations and their results are shown in Section IX. The paper concludes with remarks of Section X.

II. Mechanism Design and Game Model with Heterogeneous Users

At the center of the mechanism design model is the *designer* $\mathcal{D}$ who influences N *users*, denoted by the set $\mathcal{A}$, and participating in a **strategic (noncooperative) game**. These players are autonomous and rational decision makers, who share and compete for limited resources of the network under the given constraints of the environment. Let us define an N-player strategic game, $\mathcal{G}$, where each player $i \in \mathcal{A}$ has a respective **decision variable** x_i such that

$$x = [x_1, \ldots, x_N] \in \mathcal{X} \subset \mathbb{R}^N,$$

where $\mathcal{X}$ is the decision space of all players. Let

$$x_{-i} = [x_1, \ldots, x_{i-1}, x_{i+1}, \ldots x_N] \in \mathcal{X}_{-i} \subset \mathbb{R}^{N-1},$$

be the profile of decision variable of players other than i^{th} player and $\mathcal{X}_{-i}$ is the respective decision space. As a starting point, this paper assumes scalar decision variables and a compact and convex decision space. The decision variables may represent, in network resource allocation problems, player flow rate, power level or Signal to Interference Ratio (SINR). Due to the inherent coupling between the players, the decisions of players directly affect each other's performance as well as the aggregate allocation of limited resources.

The **preferences** of the players are captured by utility functions

$$U_i(x) : \mathcal{X} \to \mathbb{R}, \quad \forall i \in \mathcal{A},$$

which are chosen to be continuous and differentiable for analytical tractability. In this paper, the selfishness nature of users are captured by continuous and differentiable concave utility functions.

We consider here a mechanism design having heterogeneous users in the induced game, in which one subset of users have 'abnormal' utility function compared to the class of regular selfish users. The utility function of the class of malicious users can be very different depending on their nature and goals. The disrupting nature of malicious users where they want to create loss to other users even at the cost of their benefit and the altruistic nature of some users who want to care for the social welfare can be captured with a modified utility function. One such modified utility function can be obtained by a convex combination of user utilities

$$U_i^m = U_i + \theta_i \sum_{j \neq i} U_j, \tag{1}$$

where θ_i is the parameter between -1 and 1 which captures the range of behavior of a user. This utility function can be modified by taking the average of the utilities of all the users in the second term [14]. Unlike in [21], where the Degree of Cooperation of a user as a vector of values corresponding to all other users is used to model altruism, we use one scalar value θ to model the behavior of users ranging from altruism to maliciousness.

The table below lists the values of θ and corresponding user behavior.

θ	Behavior
$0 < \theta$	altruistic
$\theta = 0$	selfish
$\theta < 0$	malicious

Let us define the set of selfish users be $\mathcal{S} \subset \mathcal{A}$. Also, the set of malicious and altruistic users, i.e. users with $\theta_i \neq 0$ is defined as $\mathcal{B}$ and $\mathcal{B} = \mathcal{A} \backslash S$. When the set $\mathcal{B}$ has only malicious users, the utility function of malicious users can be modified as

$$U_i^m = U_i + \theta_i \sum_{j \in \mathcal{S}} U_j, \ \forall i \in \mathcal{B}. \tag{2}$$

Note that even if the utility function U_i is concave in x_i, the malicious user utility function U_i^m may not be concave in x_i. For concavity the utility functions should satisfy following condition,

$$\frac{d^2 U_i}{dx_i^2} + \theta_i \sum_{j \neq i} \frac{d^2 U_j}{dx_i^2} \leq 0, \forall i. \tag{3}$$

We start with general concave utility functions for the users but for the analytical results with unique NE we use the utility functions which satisfy the condition in equation (3).

We could also use the alternate utility function,

$$U_i^m = (1 - |\theta_i|) U_i + \theta_i \sum_{j \neq i} U_j, \tag{4}$$

to model the malicious behavior with a gradual decrease in the self utility when θ decreases. But this will lead to a canceling out of the effect on the selfish users in the case of network resource allocation.

The extreme selfishness or greedy nature of malicious users can be also captured with a convex utility function. In this case they will take the maximum possible share of the resource constrained above by either physical limits or a level that leads to immediate detection.

The designer $\mathcal{D}$ devises a **mechanism** M, which can be represented by the mapping $M : \mathcal{X} \to \mathbb{R}^N$, implemented by introducing incentives in the form of *rules and prices* to players. The latter can be formulated by adding it as a cost term such that the player i has the quasi-linear cost function

$$J_i(x) = c_i(x) - U_i^m(x). \tag{5}$$

where $c_i(x)$ is the price payed by i^{th} user to the mechanism.

We differentiate between two kinds of mechanisms, auctions and pricing, which differ in the assumption on nature of the users and the interaction rules. In auction mechanisms, the designer $\mathcal{D}$ imposes on a player $i \in \mathcal{A}$ a user-specific

- resource allocation rule, $Q_i(x)$,
- resource pricing, $c_i(x)$,

based on their bids x. The price anticipating users decide on their bid, minimizing their individual cost.

In pricing mechanisms, the price taking users decide on their allocation as best response to the user specific price P_i induced by the designer and there is no explicit allocation rule dictated by the designer. In this case, the cost function is

$$J_i(x) = P_i x_i - U_i(Q(x)).$$

Similar to player preferences, the **designer objective**, e.g. maximization of aggregate user utilities or social welfare, can be formulated using a smooth objective function V for the designer:

$$V(x, U_i(x), c_i(x)) : \mathcal{X} \to \mathbb{R},$$

where $c_i(x)$ and $U_i(x)$, $i = 1, \ldots, N$ are user-specific pricing terms and player utilities, respectively. Hence, the global optimization problem of the designer is simply $\max_x V(x, U_i(x), c_i(x))$, which it solves *indirectly* by setting rules and prices. The different properties of mechanisms analyzed in this paper are attached in the appendix.

In this paper, for tractability purposes, we model user i's utility function as logarithmic, parameterized by her private value α_i. In this case, the aim of the designer in the auction setting will be to make the users report their true private value, i.e, $x_i = \alpha_i$ and carry out an efficient allocation based on that.

The players share and compete for limited resources in the given environment under its information and communication constraints. We focus on two basic types of resource sharing and coupling, which are often encountered in a variety of problems in networking:

1) *Additive resource sharing:* the players share a finite resource C such that

$$\sum_{i=1}^{N} x_i = C.$$

This type of coupling is encountered in bandwidth sharing and rate control in networks.

2) *Interference coupling* (linear interference): the resource allocated to player i, γ_i, is inversely proportional to interference generated others such that

$$\gamma_i(x) = \frac{h_i x_i}{\sum_{j \neq i} h_j x_j + \sigma},$$

where $h_i \ \forall i$ and σ denote some system parameters. Interference coupling occurs in wireless networks where γ represents signal-to-interference ratio.

The altruistic user's best strategy for the above resource sharing and coupling scenarios is to take no resource and effectively be idle in the game. We assume that the malicious users have information about the utility function of other selfish users but the regular selfish users do not have the information about the existence of malicious users and their identities. We consider the case where the selfish users cannot collaborate, detect and punish malicious users themselves since it will require a lot of common information and communication for coordination. Therefore, we use a designer who anticipates and detects malicious behavior of any user and modifies the pricing appropriately to counter the malicious behavior. In the next sections, the effect of malicious users to system social welfare is quantified and some counter measures are proposed.

III. Adversarial behavior in VCG Mechanism

We assume here unlike classical VCG mechanism, instead of reporting $U_i(x)$ the malicious user reports $U_i^m(x)$ to the designer as its utility function.

A. VCG Mechanism for Divisible Resources

The total payment by an user for a divisible resource allocation is given by

$$c_i^{VCG} = -\sum_{j \neq i} U_j^m(Q_j^*(x)) + \sum_{j \neq i} U_j^m(Q_j^i(x))$$

where

$$Q^* = \arg\max_{Q} \sum_{j} U_j^m(Q_j(x))$$

and

$$Q^i = \arg\max_{Q} \sum_{j \neq i} U_j^m(Q_j(x))$$

. Now the individual cost will be

$$J_i = c_i^{VCG} - U_i^m(Q_i^*(x)).$$

Consider logarithmic utility function for the users. Then the allocation and payment would be,

$$Q_i^* = \frac{\alpha_i C}{\sum_j \alpha_j},$$

$$c_i^{VCG} = \sum_{j \neq i} \alpha_j \log\left(\frac{\sum_m \alpha_m}{\sum_{m \neq i} \alpha_m}\right)$$

Let us consider the case where user k is malicious and reports U_k^m to the designer. Then the allocation becomes

$$Q^* = \arg\max_{Q} \ (U_k(Q_k) + (1+\theta_k) \sum_{j \neq k} U_j^m(Q_j(x))).$$

Consider logarithmic utility function for the users.

$$Q^* = \arg\max_{Q} \ \alpha_k \log(Q_k) + (1+\theta_k) \sum_{j \neq k} \alpha_j \log(Q_j(x)).$$

The user allocations will be,

$$Q_k^* = \frac{\alpha_k C}{\alpha_k + (1+\theta_k)\sum_{j\neq k} \alpha_j},$$

$$Q_j^* = \frac{\alpha_j (1+\theta_k) C}{\alpha_k + (1+\theta_k)\sum_{j\neq k} \alpha_j}, \forall j \neq k$$

It can be observed that the allocation to malicious user increases and that of other users reduce when θ_k decreases from 0 towards -1 compared to the case where none of the users are malicious. Therefore the malicious user is able to destroy the efficiency property of the VCG mechanism. Also,

$$Q_k^i = \frac{\alpha_k C}{\alpha_k + (1+\theta_k)\sum_{j\neq k,i} \alpha_j}, i \neq k$$

$$Q_j^i = \frac{\alpha_j (1+\theta_k) C}{\alpha_k + (1+\theta_k)\sum_{j\neq k,i} \alpha_j}, \forall j \neq k, i$$

$$Q_j^k = \frac{\alpha_j C}{\sum_{m=k,j} \alpha_m}$$

The VCG payment for this case will be,

$$c_i^{VCGm} = \sum_{j\neq i} \alpha_j \log(\frac{\alpha_k + (1+\theta_k)\sum_{j\neq k} \alpha_j}{\alpha_k + (1+\theta_k)\sum_{j\neq k,i} \alpha_j})$$

$$c_k^{VCGm} = \sum_{j\neq k} \alpha_j \log(\frac{\alpha_k + (1+\theta_k)\sum_{j\neq k} \alpha_j}{(1+\theta_k)\sum_{m\neq k,j} \alpha_m})$$

It can be also observed that the malicious users are not made to pay proportional to the loss in efficiency they cause. Therefore, even the VCG mechanism is vulnerable to malicious behavior. In the following sections we quantify their effect of adversarial behavior in the mechanisms proposed for network resource allocation.

Here we assumed that the malicious users have full knowledge of the utility fictions of other selfish users. One way is to use learning or to adopt Bayesian approach by the malicious user.

IV. Price of Malice in Mechanisms

In this section, we quantify the robustness of mechanisms described in the above setting, against malicious players. For this purpose, we first redefine the metric Price of Malice ($PoM(M)$) of mechanism M suitable for mechanisms in resource sharing setting. A similar metric called Price of Byzantine Anarchy is used in [6] to quantify the social welfare loss at Nash equilibrium point in the presence of malicious users compared to the optimal point, but in a virus inoculation game scenario. For congestion games with malicious flow concentrated on one malicious player Price of Malice was redefined, based on the delay experienced at Nash equilibrium point with and without the malicious player in [7]. We now define PoM for network games with discrete set of players similar to the definition given in [7].

Definition IV.1. *The metric Price of Malice(PoM) of a mechanism M is defined as:*

$$PoM(M) := \frac{\sum_{j\in\mathcal{S}} U_j(Q_j(x)) - \sum_{j\in\mathcal{S}} U_j(Q'_j(x))}{\sum_{j\in\mathcal{S}} U_j(Q_j(x))},$$

where Q is the allocation at the Nash equilibrium when none of the users are malicious and Q' is the allocation at the Nash equilibrium in the presence of malicious users.

Now, we estimate the value of Price of Malice parameter for two networks which differ in user coupling and resource sharing as described in the previous section.

A. Price of Malice in Auction Mechanisms

We present auction mechanisms [31] for two network coupling schemes, rate control in wired networks and power allocation in interference coupled wireless networks, and quantify the Price of Malice for both cases. The adversarial behavior considered

in this section is that the malicious players take maximum possible share of the resources and hence try to disrupt others by denying them their fair share of resources.

Additive Sharing (Rate Control in Networks)

We consider the rate sharing problem with users having separable utility in networks and quantify the effect of the adversarial behavior on it. Let users with utilities $U_i(Q_i)$ share a fixed bandwidth C such that $\sum_{i=1}^{N} Q_i(x) = C$, where $x_i \in (0, x_{max})$. The vector x in this case denotes player flow rates and Q the capacity allocated to them [32], [33]. Consider the utility function given in (6) and the cost of i^{th} user is given by,

$$J_i^m = c_i - U_i - \theta_i \sum_{j \in \mathcal{S}} U_j, \forall i. \tag{6}$$

We need to check whether the user cost functions are convex. The total price part of the cost function is ensured to be convex in the mechanisms we consider in this paper. For the cost function to be convex in x_i, the utility part should be also convex. This says that the utility functions, should satisfy the condition given in (3).

For malicious users, if the cost function is convex under the above condition and best response can be obtained from the first order conditions. Since all the user cost functions are convex, the best response points obtained from first order conditions give Nash equilibrium.

The designer solves the constrained optimization problem

$$\max_Q V(Q) \Leftrightarrow \max_Q \sum_i U_i(Q_i) \text{ such that } \sum_i Q_i = C, \tag{7}$$

in order to find a globally optimal allocation Q that satisfies this **efficiency criterion**. The associated Lagrangian function is then

$$L(Q) = \sum_i U_i(Q_i) + \lambda \left(C - \sum_i Q_i \right),$$

where $\lambda > 0$ is a scalar Lagrange multiplier. Under the convexity assumptions made, this leads to

$$\frac{\partial L}{\partial Q_i} \Rightarrow U_i'(Q_i) = \lambda, \ \forall i \in \mathcal{A}, \tag{8}$$

and the efficiency constraint

$$\frac{\partial L}{\partial \lambda} \Rightarrow \sum_i Q_i = C. \tag{9}$$

and $Q_i = 0$ for users with $U_i'(Q_i) < \lambda$.

Let the designer employ the total payment to i^{th} user as the one obtained in [18] assuming all the users are just selfish in an efficient auction mechanism M_a with proportional allocation which is defined based on the bid of player i,

$$Q_i := \frac{x_i}{\sum_j x_j + \omega} C. \tag{10}$$

After deriving the allocation rule, we next design the pricing rule/function. For this we resort to use of a generator function, as in [18]. Let us define $t = \sum_j x_j + \omega$ is a measure of demand for the resource and which allows us to characterize agent optimal responses with respect to a parameter which is identical for all agents at equilibrium. The generator function is $g(.)$ is a function of t to $\mathbb{R}^+$ and plays the role of Lagrange multiplier to generate the optimal pricing function. The total payment of i^{th} user has several choices, depending on the choice of generator function.

For $g(t) = t^2$,the payment function is derived in [18] as

$$c_i = x_i \sum_{j \neq i} x_j + \omega \tag{11}$$

which is convex payment function and is sufficient to guarantee a unique Nash equilibrium.

Let us check for the special case of logarithmic utilities, i.e, $U_i(Q_i) = \alpha_i \log Q_i(x)$. Consider the mechanism M_a.

Proposition IV.2. *The Nash equilibrium point of the mechanism M_a with logarithmic utilities is given as*

$$x_i^* = \frac{\alpha_i}{t(1+\theta_i)C},$$

where $-1 < \theta \leq 1$.

Proof: By substituting the payment function of the mechanism M_a given in (11) in the cost function given in equation (6) we obtain a convex cost for all the users. This guarantees a unique NE of the mechanism [34] which can be obtained from the first order conditions. The best response of user becomes

$$\frac{\partial J_i^m}{\partial x_i} = 0 \Longrightarrow x_i^* = \frac{\alpha_i}{t(1+\theta_i)C},$$

by using the fact that selfish users will have the Nash equilibrium point $x_i^* = \frac{\alpha_i}{tC}$, from the incentive compatibility property of the mechanism. ■

We can observe that malicious users having $-1 < \theta < 0$, will have the Nash equilibrium point as $x_i^* > \frac{\alpha_i}{tC}$. Therefore, the malicious users bid higher than the selfish users. The allocation for the regular selfish users, i.e., users with $\theta_i = 0$ in the presence of malicious users can be written as

$$Q_i' = \frac{\frac{\alpha_i}{tC}C}{\sum_{j\in\mathcal{S}} \frac{\alpha_j}{tC} + \sum_{k\in\mathcal{B}} \frac{\alpha_k}{t(1+\theta_k)C}}. \tag{12}$$

Let

$$r_i = \frac{Q_i}{Q_i'} = \frac{\sum_{j\in\mathcal{S}} \alpha_j + \sum_{k\in\mathcal{B}} \frac{\alpha_k}{(1+\theta_k)}}{\sum_j \alpha_j} \tag{13}$$

be the ratio of allocation of selfish users before and after the presence of malicious users. Now we obtain the value of PoM of the mechanism M_a at the NE point given in Proposition IV.2.

Proposition IV.3. *For th additive resource sharing case, the Price of Malicious $PoM(M_a)$ is*

$$PoM(M_a) = \frac{\sum_{j\in\mathcal{S}} \alpha_j \log(r_j)}{\sum_{j\in\mathcal{S}} \alpha_j \log(\frac{\alpha_j C}{\sum_i \alpha_i})}.$$

For the case where users are symmetric $\alpha_i = \alpha,\ \forall i$, and only one user is malicious or all the malicious user coordinate to form one entity, this simplifies to

$$PoM(M_a) = \frac{\log(\frac{N-1+\frac{1}{1+\theta_k}}{N})}{\log(\frac{C}{N})}.$$

Proof: The results follow directly by using the allocation given in equation (24) and the value of r_i in equation (13) to the definition of PoM in Definition IV.1. ■

In the case of presence of malicious users, as θ decreases from 0 to -1, we can see that the $PoM(M_a)$ increases. We could observe that the $PoM(M_a)$ cannot be bounded for different possible values of θ_k and is unbounded when θ_k reaches -1.

We also present another auction-based mechanism, $\mathcal{M}_a'$, for the case when the bid is equal to the payment. The approximately efficient, mechanism, $\mathcal{M}_a'$, can be defined based on the bid of player i as,

$$x_i := P_i(x)Q_i(x), \tag{14}$$

the pricing function

$$P_i := \frac{\sum_{j\neq i} x_j + \omega}{C}, \tag{15}$$

for a scalar $\omega > 0$ sufficiently large such that $\sum_i Q_i \leq C$, and the resource allocation rule

$$Q_i := \frac{x_i}{\sum_{j\neq i} x_j + \omega} C. \tag{16}$$

It is also possible to interpret the scalar ω as a *reserve bid* [35].

Consider now the mechanism M_a' for the logarithmic case. The cost function in this case is,

$$J_i^m = x_i - \alpha_i \log(\frac{x_i}{I_i}) - \theta_i \sum_{j\in\mathcal{S}} \alpha_j \log(\frac{x_j}{I_j}),$$

where $I_i = \sum_{j\neq i} x_j + \omega$. The best responses of each user will lead to a set of equations,

$$\frac{\alpha_i}{x_i} = 1 - \theta_i \sum_{j\in\mathcal{S}} \frac{\alpha_j}{x_i + \sum_{k\notin i,j} x_k}, \forall i.$$

We can see that for the selfish users, $x_i = \alpha_i$. Therefore, for the case in which there is a single malicious user, the following polynomial of N^{th} degree is solved by the malicious user i,

$$\frac{\alpha_i}{x_i} = 1 - \theta_i \sum_{j \in \mathcal{S}} \frac{\alpha_j}{x_i + \sum_{k \notin i,j} x_k}.$$

A unique Nash equilibrium point could be obtained from the intersection of all these points due to the convexity of the cost function. But it is not possible to have analytical result for the NE in this case. As above, the PoM can be calculated in this case also but numerically. Therefore, the variation of values of $PoM(M_a')$ for different values of θ is given in the simulation section.

From the above equations, we can see that the Price of Malice of a mechanism can be obtained knowing system parameters and user preferences and can be bounded above and below (if possible) depending on the range and distribution of these values for the specific setting.

Interference Coupled Systems (CDMA Power Control)

Consider an auction mechanism in the context of a wireless network and uplink power control setting ([35], [36]) where due to the interference coupling the resource sharing is inherently competitive. Let the user utilities be defined as $U_i(x) = \alpha_i \log \gamma_i(Q(x))$ and the individual power levels, Q, satisfy $\sum_{i=1}^{N} Q_i \leq C$, where the signal-to-interference ratio (SINR) received by the base station is

$$\gamma_i = \frac{Q_i(x)}{\sum_{j \neq i} Q_j(x) + \sigma},$$

and $x_i \in (0, x_{max})$.

An auction-based mechanism, $\mathcal{M}_b$, can be defined based on the bid of player i, with the resource allocation rule

$$Q_i := \frac{x_i}{\sum_j x_j} C, \tag{17}$$

which is proportional allocation as first analyzed in [18]. We can see that using this proportional allocation, full utilization of resource is attained, i.e. $\sum_i Q_i = C$. Now we decouple the user utilities by rewriting γ_i as

$$\gamma_i(Q_i) = \frac{Q_i(x)}{C - Q_i(x) + \sigma}, \tag{18}$$

using the full utilization property. For the allocation given in (17), the SINR is

$$\gamma_i(x) = \frac{x_i C}{\sum_j x_j (C + \sigma) - x_i C}. \tag{19}$$

In [35], it is observed that in systems with sufficiently high SINR assumption $U_i(x) = \alpha_i \log \gamma_i(Q_i(x))$ is concave in Q_i, where $\gamma_i(Q_i)$ is given by (18). A pricing mechanism given in equation 11 will make the selfish users to report $x_i = \alpha_i$.

In the presence of malicious and altruistic users the SINR obtained by the regular users will be,

$$\gamma_i'(x) = \frac{\alpha_i C}{(\alpha^s + \sum_{k \in \mathcal{B}} \frac{\alpha_k}{1 + \theta_k})(C + \sigma) - \alpha_i C} \tag{20}$$

where $\alpha^s = \sum_{j \in \mathcal{S}} \alpha_j$. Now we give the value of $PoM(M_b)$ in the following proposition.

Proposition IV.4. *The PoM of the mechanism M_b for the interference coupled wireless system is given as*

$$PoM(M_b) = \frac{\sum_{j \in \mathcal{S}} \alpha_j \log(\frac{\gamma_j}{\gamma_j'})}{\sum_{j \in \mathcal{S}} \alpha_j \log(\frac{\alpha_j C}{\sum_k \alpha_k (C+\sigma) - \alpha_j C})}.$$

In the symmetric case if only one user is malicious, the PoM becomes

$$PoM(M_b) = \frac{\log(\frac{(N - 1 + \frac{1}{1+\theta_k})(C+\sigma) - C)}{N(C+\sigma) - C})}{\log(\frac{C}{N(C+\sigma) - C})}.$$

A similar behavior of $PoM(M_b)$ as in the case of additive sharing can be observed for different values of θ. The variation of $PoM(M_b)$ for different values of θ is given in the simulation section for a specific set of parameters.

B. Price of Malice in Pricing Mechanisms

In pricing mechanisms the users choose their allocation as their strategy or action and do not simply report their valuations unlike in auction mechanisms. Therefore, pricing mechanisms are indirect mechanisms. Their actions reveal only some information about their utility function. The pricing mechanisms are more appropriate for modeling distributed systems where we cannot expect a central authority to allocate resource to the users.

A counterpart of the Price of Malice metric in Definition IV.1 for pricing mechanisms [15], which differ from auctions by their lack of an explicit resource allocation scheme, can be obtained by replacing $Q(x)$ and $Q'(x)$ with the action vector without malicious users x and with malicious users x', respectively.

In the case of additive resource sharing, the users with utilities $U_i(x_i) = \alpha_i \log x_i$ share the fixed resource $\sum_{i=1}^{N} x_i = C$, and $x_i \in (0, x_{max})$. Consider an efficient mechanism M_c, which can be implemented in an iterative way. The efficient allocation is

$$x_i = \frac{\alpha_i}{\lambda},$$

where λ is the Lagrange multiplier. In the case of all selfish users $\lambda = \sum_i \alpha_i / C$ and it will be set as price to the users.

We can observe that in the case of pricing, the utility function of the malicious user is given by,

$$J_i^m = P_i(x)x_i - U_i(x_i) - \theta_i \sum_{j \in \mathcal{S}} U_j(x_j).$$

We can see that the additional third term does not have direct dependence on x_i and does not play a role in malicious user cost minimization. But, that term is indirectly a function of x_i due to the additive coupling in the global objective. The effect of the additive coupling in the global objective is brought by Lagrange multiplier which acts as the price in the user objective.

Let each malicious user take a share x_m which can be x_{max}, the maximum share they can use without detection, according to their utility function, in order to disrupt others. Let λ' be the Lagrange multiplier in this case which will be a different point than $\lambda = \sum_i \alpha_i / C$. The remaining resource $(C - \sum_{\mathcal{B}} x_m)$ will be shared among good users, under the efficient mechanism M_c.

Proposition IV.5. *In the additive sharing case $PoM(M_c)$ is,*

$$PoM(M_c) = \frac{\sum_{j \in \mathcal{S}} \alpha_j \log(\frac{C\lambda'}{\sum_i \alpha_i})}{\sum_{j \in \mathcal{S}} \alpha_j \log(\frac{\alpha_j C}{\sum_i \alpha_i})}.$$

For symmetric case, where $\alpha_i = \alpha \; \forall i$, it becomes

$$PoM(M_c) = \frac{\log(\frac{C\lambda'}{N\alpha})}{\log(\frac{C}{N})}.$$

A Nash Equilibrium is the equilibrium point of the above mechanisms for the pricing schemes in the presence of malicious users. It is possible to iteratively compute the NE solution either using best responses of users or adopting a gradient algorithm. Gradient algorithms often have better convergence properties. Hence, we present a distributed iterative scheme. We assume that the users instead of jumping directly to the Nash equilibrium take gradient best response. The dynamics of the user behavior assuming the users are bounded rational is given below. All the users including malicious ones take gradient best response with respect to their cost function in dynamics given by the iterative algorithm. The iterative distributed mechanism is given in [37] as,

$$x_i(k+1) = x_i(k) - \kappa_i \frac{\partial J_i}{\partial x_i} \;\; \forall i \in \mathcal{S}, \tag{21}$$

$$x_i(k+1) = x_i(k) - \kappa_i^m \frac{\partial J_i^m}{\partial x_i} \;\; \forall i \in \mathcal{B}, \tag{22}$$

$$\lambda(k+1) = \lambda(k) + \kappa_D \big(\sum_i x_i(k+1) - C \big). \tag{23}$$

The malicious user observing the action of selfish users, updates its action. The malicious user updated action affects the λ update by the designer.

The counterpart of auction in the interference-coupled case for pricing can be obtained in a similar way and the mechanism can be denoted as M_d. The variation of values of $PoM(M_c)$ and $PoM(M_d)$ for different number of users is given and compared with each other in the simulation section.

C. Additional metrics to quantify the effect of malicious behavior

Here we introduce additional metric definitions to quantify the effect of malicious behavior. Our PoM definition is similar to the externality-price definitions in [26] in the context of altruistic behavior, since we quantify the effect of malicious players on selfish players. Social Maliciousness Price:

Definition 1. **Social Maliciousness Price(SMP):** The ratio between the social welfare of players, at equilibrium before and after the presence of malicious players.

$$SMP(M) := \frac{\sum_{j\in\mathcal{A}} U_j(Q'_j(x))}{\sum_{j\in\mathcal{A}} U_j(Q_j(x))},$$

The allocation for malicious users and social welfare with the presence of malicious users in the set $\mathcal{B}$ would be:

$$Q'_k = \frac{\frac{\alpha_i}{tC}C}{\sum_{j\in\mathcal{S}}\frac{\alpha_j}{tC} + \sum_{k\in\mathcal{B}}\frac{\alpha_k}{t(1+\theta_k)C}}. \tag{24}$$

$$SW^m = \sum_{j\in\mathcal{S}} \alpha_j \log(\frac{\alpha_j C}{\sum_{j\in\mathcal{S}}\alpha_j + \sum_{k\in\mathcal{B}}\frac{\alpha_k}{(1+\theta_k)}}) + \sum_{k\in\mathcal{B}} \alpha_k \log(\frac{\frac{\alpha_k}{(1+\theta_k)}C}{\sum_{j\in\mathcal{S}}\alpha_j + \sum_{k\in\mathcal{B}}\frac{\alpha_k}{(1+\theta_k)}})$$

In the case one user is malicious user among all symmetric users, the social welfare will turn out to be

$$SW^m = \alpha \log(\frac{(1+\theta_k)^{N-1}C^N}{((N-1)(1+\theta_k)+1)^N})$$

The social welfare with all selfish symmetric users is,

$$SW = \alpha \log(\frac{C^N}{N^N})$$

Therefore, the social welfare with malicious user is higher if the value of θ_k satisfies the following inequality.

$$(1+\theta_k)^{N-1} > (\frac{(N-1)(1+\theta_k)+1}{N})^N$$

For example with $\theta_k = \frac{-1}{2}$ the above inequality holds for all the values of $N > 2$. This is a Braess type paradox since the presence of a malicious user improves the social welfare. But it should be noted that this higher social welfare happens at the expense of the utility of the regular users.

Definition 2. **Individual Maliciousness Price(IMP):** The ratio between the total utility of malicious players , at equilibrium before and after they become malicious players.

$$IMP(M) := \frac{\sum_{j\in\mathcal{B}} U_j(Q'_j(x))}{\sum_{j\in\mathcal{B}} U_j(Q_j(x))},$$

The value of this metric for a mechanism can be easily obtained from the value of PoM and SMP. Since the malicious players always have more utility by being malicious this metric does not create any paradox.

D. Price of Malice of Mechanism with Malicious User Interested in Payment of Selfish Users

In some scenarios, the malicious user would like to make other users pay more in addition to reduce the share of their resource [38]. Here we consider the kind of malicious users who are interested in the total cost of the selfish users, i.e, she want to affect the payment along with the resource allocation of the selfish users. The cost of the malicious user in this case is redefined as,

$$J_i^m = J_i - \theta_i \sum_{j\in\mathcal{S}} J_j,$$

where $J_i = c_i - U_i$, is the regular cost of a user.

Additive Sharing (Rate Control in Networks): Let us take the case of mechanism M_a and logarithmic utilities for the users. For this case, the cost of the malicious user becomes,

$$J_i^m = x_i I_i - \alpha_i \log(\frac{x_i}{x_i + I_i}) - \theta_i \sum_{j\in\mathcal{S}} (x_j I_j - \alpha_j \log(\frac{x_j}{x_i + I_i}),$$

From the first order conditions we obtain the Nash equilibrium point as $x_i = \frac{\alpha_i}{t(1+2\theta_i)}$. We can see that the malicious user over bid than his type α, as $-\frac{1}{2} < \theta_i < 0$ to affect the regular users. We can obtain the price of malice for this case as in Section VIII.

V. Convergence Analysis of Iterative Distributed Algorithm

In this section we analyze the convergence of the iterative distributed algorithm defined by equations (21), (22) and (23) in the previous section.

Theorem V.1. *In the iterative pricing mechanism $\mathcal{M}^a$ in the Section IV defined by the set of equations (21), (22) and (23) converges to a unique point in the constraint set individually if $0 < \kappa_i < \frac{2}{M_1}, \forall i$, $0 < \kappa_i^m < \frac{2}{M_m}, \forall i$ and $0 < \kappa_D < \frac{2}{M_2}$, where M_1 is the constant which bounds $||D(\delta J_i(x))||, \forall x \in S$, M_m is the constant which bounds $||D(\delta J_i^m(x))||, \forall x \in S$ M_2 is the constant which bounds $||D(\delta L(\lambda))||, \forall \lambda \in R_n^+$ and D is the Jacobian matrix. The algorithm converges to a unique point assuming that the Lagrange multiplier update in (23) happens in a slower time scale than the user action updates in (21) and (22).*

Proof: In [39], for analyzing constraint optimization problems, the infeasible points are projected back to the feasible region. The projection mapping is defined as,

$$[x]^+ = \arg\min_{z \in S} ||z - x||_2$$

where S is the feasible set.

For the convergence of the gradient projection algorithm the relaxations of Assumptions 3.1 given in [39] (pp. 213) are to be satisfied as sufficient conditions. The relaxed Assumption 1 says that $F(x) > c, \forall x \in S$ for a $c \in R$ for any F to be minimized. Both user cost function and the global objective satisfy this. The second assumption is Lipschitz continuity condition given by,

$$||\delta J_i(x) - \delta J_i(y)|| \leq K||x - y||, \forall x, y \in S.$$

The user cost function are twice continuously differentiable due to the presence of noise term in the denominator of the interference term. Therefore, we can use the mean value theorem for vector valued functions which states that,

$$\delta J_i(x) - \delta J_i(y) = (\int_0^1 D(\delta J_i(y + t\rho)dt)) \cdot (x - y), \forall x, y \in S, \forall i$$

where $\rho = x - y \in X$, $0 \leq t \leq 1$ and D is the $N \times N$ Jacobian matrix. The Jacobian matrix D is defined as,

$$D(\delta J_i(x)) := \begin{pmatrix} c_1 & c_{12} & \cdots & c_{1N} \\ c_{21} & c_2 & \cdots & c_{2N} \\ \vdots & & \ddots & \vdots \\ c_{N1} & c_{N2} & \cdots & c_N \end{pmatrix}, \tag{25}$$

where $c_m := \frac{\partial^2 J_i}{\partial x_m^2}$ and $c_{lk} := \frac{\partial^2 J_i}{\partial x_l \partial x_m}$.

Using the Cauchy-Schwartz inequality,

$$||\delta J_i(x) - \delta J_i(y)|| \leq M_1||x - y||, \forall x, y \in S, \forall i, \tag{26}$$

where M_1 is the constant which bounds $||D(\delta J_i(x))||, \forall x \in S$. The set S is convex and $(y + t\rho) \in S$ for t between 0 and 1. For $x \in S$, M_1 is bounded when the boundaries of S are finite. Similarly, we can define M_m as the constant which bounds $||D(\delta J_i^m(x))||, \forall x \in S$. Therefore, the action update according to equations (21) and (22) converges if $0 < \kappa_i < \frac{2}{M_1}, \forall i \in \mathcal{S}$ and $0 < \kappa_i^m < \frac{2}{M_m}, \forall i \in \mathcal{B}$ for given λ and thus prices.

Here we do the distributed implementation by the alignment of users and designer problems. When the designer updates the prices according to (21),

$$\frac{dJ_i}{dx_i} = -\frac{dV}{dx_i}.$$

Therefore, the gradient update in (21) is according to the gradient update of the global objective.

The Lagrange function of the global objective is given by

$$L = \sum_i w_i U_i(\gamma_i(x)) - \sum_i \lambda_i(\frac{x_i}{h_i} - P_{max}).$$

subject to the condition that $\lambda_i \geq 0, \forall i$. The gradient descent equation for L is given by

$$\lambda_i(k+1) = [\lambda_i(k) + \kappa_D \frac{\partial L}{\partial \lambda_i}]^+ \ \ \forall i \tag{27}$$

The equation (22) is equivalent to equation (23).

Also, we need to prove the Lipschitz continuity of the Lagrange function of global objective w.r.t. the λ vector also. From the mean value theorem,

$$\begin{aligned} \delta L(\lambda^{(1)}) - \delta L(\lambda^{(2)}) &= (\int_0^1 D(\delta L(\lambda^{(2)} + t\nu)dt)) \\ &\cdot \ (\lambda^{(1)} - \lambda^{(2)}), \ \forall \lambda^{(1)}, \lambda^{(2)} \in R_+^n \end{aligned}$$

and

$$||\delta L(\lambda^{(1)}) - \delta L(\lambda^{(2)})|| \leq M_2 ||\lambda^{(1)} - \lambda^{(2)}||, \forall \lambda^{(1)}, \lambda^{(2)} \in R_+^n.$$

Therefore, the Lagrange multiplier update according to equation (23) converges if $0 < \kappa_D < \frac{2}{M_2}$, for given action vector. Gradient descent equations under the above assumptions converges according to Prop. 3.4. in [39] (pp. 214).

Since user cost function and Lagrange function of the global objective are convex, the equations converges to a unique point in the constraint set according to Prop. 3.5 in [39].

The action update happens in a faster timescale and it converges for any given value of the Lagrange multiplier. Lagrange multiplier update happens in the direction of global optimum once in several time step of the action update. Therefore, the algorithm converges to a unique point.

Hence proved. ■

VI. Collusion behavior in Network Mechanisms

Some of the (malicious) players can form a collusion(group of players) to manipulate the network mechanisms by carefully coordinating their actions in order to minimize their individual cost. A mechanism is group strategy-proof if it can resist this group forming tendency of players to cheat the designer. In this section, we investigate group strategy-proofness of a particular mechanism. Also some metrics are defined to quantify the effect of collusion and expressions are obtained for some of them in this section.

A. Group Strategy-proofness of Mechanisms

We analyze group strategy-proofness of the mechanism M_a' defined above and check whether the approximately efficient and strategy-proof mechanism M_a' proposed is ϵ-group strategy-proof.

Theorem VI.1. *The mechanism M_a' is ϵ-group strategy-proof and*

$$\epsilon = \max_{k \in \mathcal{E}} \alpha_k (\frac{\tau_k^2 - \tau_k^3}{\tau_k^2 - \tau_k + 1}), \tag{28}$$

where

$$\tau_k = \frac{(m-1)\alpha_k}{\sum_{j \neq k} \alpha_j + \omega}$$

and $\mathcal{E} = \{j : \tau_j < 1\}$.

Proof: Consider m adversarial users out of N total form a coalition $\mathcal{C}$ to cheat the system. Let us take that the bid from these agents be $\tilde{x}_k = x_k + \delta$. Now the allocation will be,

$$\tilde{Q}_k = \frac{x_k + \delta}{\sum_{j \neq k} x_j + (m-1)\delta + \omega} C, \ \forall \ k \in \mathcal{C}$$

and

$$Q_i = \frac{x_i}{\sum_{j \neq i} x_j + m\delta + \omega} C, \ \forall \ k \in \mathcal{A} \backslash \mathcal{C}.$$

We obtain costs as,

$$\tilde{J}_k = x_k + \delta - \alpha_k \log(\frac{x_k + \delta}{\sum_{j \neq k} x_j + (m-1)\delta + \omega} C) \forall \ k \in \mathcal{C}.$$

The condition for ϵ-group strategy-proofness is

$$J_k - \tilde{J}_k \leq \epsilon, \ \forall \ k \in \mathcal{C}.$$

$$
\begin{aligned}
J_k - \tilde{J}_k &= \alpha_k \log\left(\frac{x_k}{\sum_{j\neq k} x_j + \omega} C\right) \\
&- \delta + \alpha_k \log\left(\frac{x_k + \delta}{\sum_{j\neq k} x_j + (m-1)\delta + \omega} C\right) \\
&\leq \epsilon, \ \forall \ k \in \mathcal{C}. \qquad (29)
\end{aligned}
$$

This gives,

$$
(1 + \frac{\delta}{x_k})(\frac{1}{1 + \frac{(m-1)\delta}{\sum_{j\neq k} x_j + \omega}}) \leq \exp^{\frac{\delta+\epsilon}{\alpha_k}} \ \forall \ k \in \mathcal{C}.
$$

From the utility function and resulting best response criteria, the true bid of the users is $x_k = \alpha_k$. Thus the group strategy-proof condition for this mechanism is,

$$
(1 + \frac{\delta}{\alpha_k})(\frac{1}{1 + \frac{(m-1)\delta}{\sum_{j\neq k} \alpha_j + \omega}}) \leq \exp^{\frac{\delta+\epsilon}{\alpha_k}} \ \forall \ k \in \mathcal{C}.
$$

Let us denote, $\mu = \frac{\delta}{\alpha_k}$ and

$$
\frac{(m-1)\alpha_k}{\sum_{j\neq k} \alpha_j + \omega} = \tau_k.
$$

Let us check above condition for different cases.

1) Case 1, $\mu > 0$: It can be observed that, for $\mu > 0$,

$$
\frac{1+\mu}{1+\mu\tau_k} \leq (1+\mu) < \exp^{\mu}.
$$

Thus for $\mu > 0$, $\epsilon = 0$.

2) Case 2, $\mu \leq 0$: It can be noted that, if $\mu \leq 0$, then $0 \leq |\mu| \leq 1$ because the bid from agents $\tilde{x}_k = x_k + \delta$ should be always positive. Thus, for $-1 \leq \mu \leq 0$, in the symmetric case the $\epsilon-$ group strategyproof condition becomes

$$
\frac{1-|\mu|}{1-\mu|\tau_k|} \leq \exp^{-|\mu|} \exp^{\frac{\epsilon}{\alpha_k}}.
$$

This can be rewritten as

$$
\exp^{|\mu|} \frac{1-|\mu|}{1-\mu|\tau_k|} \leq \exp^{\frac{\epsilon}{\alpha_k}}.
$$

For a given value of τ_k, maximum value of left hand side is achieved when

$$
\mu = \frac{\tau_k}{\tau_k^2 - \tau_k + 1}.
$$

By substituting this value in the above equation, it becomes

$$
\exp^{\frac{\tau_k}{\tau_k^2-\tau_k+1}}(1-\tau_k) \leq \exp^{\frac{\epsilon}{\alpha_k}}.
$$

It can be observed that for $\tau_k \geq 1$, above condition is satisfied for $\epsilon = 0$. For $\tau_k < 1$, we know that,

$$
\exp^{\frac{\tau_k}{\tau_k^2-\tau_k+1}}(1-\tau_k) < \exp^{\frac{\tau_k}{\tau_k^2-\tau_k+1}} \exp^{-\tau_k}.
$$

Thus the value of ϵ is obtained as,

$$
\epsilon = \max_{k\in\mathcal{E}} \alpha_k (\frac{\tau_k^2 - \tau_k^3}{\tau_k^2 - \tau_k + 1})
$$

where $\mathcal{E} = \{j : \tau_j < 1\}$.

Hence proved. ■

B. Price of Collusion

In [25], the Price of Collusion is defined for any game G is at most the maximum price of anarchy of G(P) over all coalitions P. In other words, the worst possible ratio between the social cost at equilibrium before and after the collusion scenario.

$$
PoC(M) := \max_{B} \frac{\sum_{j\in\mathcal{A}} U_j(Q_j^c(x))}{\sum_{j\in\mathcal{A}} U_j(Q_j(x))},
$$

where Q_j^c is the allocation after the collusion formation. Let us consider also alternate definitions of Price of Collusion like different Collusion Prices defined in [26]. We didn't quantify the effect of collusion on the network games and mechanisms, we checked only if they are resistant to collusion. The quantities defined in these previous works can be computed in our framework.

Definition 3. **Individual Collusion Price (ICP):** is defined as the worst possible ratio between the total cost of players who collude at equilibrium before and after the collusion scenario.

$$ICP(M) := \max_{\mathcal{C}} \frac{\sum_{j\in\mathcal{C}} U_j(Q_j^c(x))}{\sum_{j\in\mathcal{C}} U_j(Q_j(x))},$$

Definition 4. **Collusion Externality Price (CEP):** is defined as the worst possible ratio between the total cost of players who collude at equilibrium before and after the collusion scenario.

$$CEP(M) := \max_{\mathcal{C}} \frac{\sum_{j\in\mathcal{S}} U_j(\tilde{Q}_j(x))}{\sum_{j\in\mathcal{S}} U_j(Q_j(x))},$$

Consider m adversarial users out of N total form a coalition $\mathcal{C}$ to cheat the system. Let us take that the bid from these agents be $\tilde{x}_k = x_k + \delta$. Now the allocation will be,

$$\tilde{Q}_k = \frac{x_k + \delta}{\sum_{j\neq k} \alpha_j + (m-1)\delta + \omega} C, \ \forall \ k \in \mathcal{C}$$

and

$$Q_i = \frac{x_i}{\sum_{j\neq i} \alpha_j + m\delta + \omega} C, \ \forall \ k \in \mathcal{A}\backslash\mathcal{C}.$$

The utility obtained by each user in the collusion using $x_k = \alpha_k$is,

$$\tilde{U}_k = \alpha_k \log(\frac{\alpha_k + \delta}{\sum_{j\neq k} \alpha_j + (m-1)\delta + \omega} C) \forall \ k \in \mathcal{C}.$$

$$ICP(M) := \frac{\sum_{k\in\mathcal{C}} \alpha_k \log(\frac{\alpha_k+\delta}{\sum_{j\neq k} \alpha_j + (m-1)\delta + \omega} C)}{\sum_{k\in\mathcal{C}} \alpha_k \log(\frac{\alpha_k C}{\sum_{j\neq k} \alpha_j + \omega})},$$

It is easy to see that if the size of the collusion is sufficiently high, the colluding users have less total utility than what they have before collusion. The condition on the size of collusion is,

$$m > \frac{(\sum_{j\neq k} \alpha_j + \omega)}{\alpha_k} + 1 \tag{30}$$

For our mechanism if the malicious users form a collusion and bid higher individually they loose individually by having higher cost if the mechanism is group strategyproof from equation (27). But the above expression says as a collusion they have less total utility for certain values of size of collusion.

VII. Learning Utility Functions by Malicious Users

In the previous sections we assumed that the malicious users have knowledge of the utility functions and parameters of the selfish users. In this section, we examine one way using which the malicious user can have knowledge of the utility functions and can pose threat to the other selfish users. We study the process of learning the utilities of the selfish users by a malicious user. The malicious user learns the utility functions of each selfish user using their best response bids or actions as data points. In pricing mechanisms, the price taking players take best response actions to the the price charged by the designer. We consider the case where the malicious users use the Gaussian process regression learning to approximate the utility function of players from their actions, which are considered to be the input data points. Once the marginal utilities of players are learned, the space of the Lagrange multiplier of the total resource constraint in the designer problem is searched to obtain the optimal point. In auctions the players bid as a response to the price and allocation designed by the designer. In a similar way as in pricing, the marginal utilities are learned through Gaussian process regression. Then, the reserve bid parameter in the price and allocation functions is updated until the optimality conditions are satisfied.

We consider two specific examples of concave, non-decreasing utility functions of selfish users in order to demonstrate the results,

1) ϕ-Utility function, i.e.,

$$U_i(x_i;\alpha_i) = \begin{cases} \alpha_i \frac{x_i^{(1-\phi)}-1}{1-\phi}, & \text{if } \phi \geq 0 \text{ and } \phi \neq 1 \\ \alpha_i \log(x_i), & \text{if } \phi = 1 \end{cases}$$

2) Exponential:

$$U_i = 1 - e^{-\alpha_i x_i} \ \ \forall i \in \mathcal{A}.$$

We note however that the presented approach is applicable to any non-parametric utility function that satisfies the assumptions described above. The techniques are also independent whether the utility functions are concave or not and separable or non-separable. Therefore, the approach in this case can be generalized to a more general case.

We use Gaussian Process (GP) regression techniques in this paper. A Gaussian Process (GP) is formally defined as a collection of random variables, any finite number of which have a joint Gaussian distribution. It is completely specified by its mean function $m(x)$ and covariance function $C(x, \tilde{x})$, where

$$m(x) = E[\hat{f}(x)]$$

and

$$C(x, \tilde{x}) = E[(\hat{f}(x) - m(x))(\hat{f}(\tilde{x}) - m(\tilde{x}))], \ \forall x, \tilde{x} \in \mathcal{D}.$$

Let us for simplicity choose $m(x) = 0$. Then, the GP is characterized entirely by its covariance function $C(x, \tilde{x})$. Since the noise in observation vector y is also Gaussian, the covariance function can be defined as the sum of a *kernel function* $Q(x, \tilde{x})$ and the diagonal noise variance

$$C(x, \tilde{x}) = Q(x, \tilde{x}) + \sigma I, \ \forall\, x, \tilde{x} \in \mathcal{D}, \tag{31}$$

where I is the identity matrix. While it is possible to choose here any (positive definite) kernel $Q(\cdot, \cdot)$, one classical choice is

$$Q(x, \tilde{x}) = \exp\left[-\frac{1}{2}\left\|x - \tilde{x}\right\|^2\right]. \tag{32}$$

Note that GP makes use of the well-known *kernel trick* here by representing an infinite dimensional continuous function using a (finite) set of continuous basis functions and associated vector of real parameters in accordance with the *representer theorem*.

The training set $(\mathcal{D}, y)$ is used to define the corresponding GP, $\mathcal{GP}(0, C(\mathcal{D}))$, through the $M \times M$ covariance function $C(\mathcal{D}) = Q + \sigma I$, where the conditional Gaussian distribution of any point outside the training set, $\bar{y} \in \mathcal{X}, \bar{y} \notin \mathcal{D}$, given the training data $(\mathcal{D}, t)$ can be computed as follows. Define the vector

$$k(\bar{x}) = [Q(x_1, \bar{x}), \ldots Q(x_M, \bar{x})] \tag{33}$$

and scalar

$$\kappa = Q(\bar{x}, \bar{x}) + \sigma. \tag{34}$$

Then, the conditional distribution $p(\bar{y}|y)$ that characterizes the $\mathcal{GP}(0, C)$ is a Gaussian $\mathcal{N}(\hat{f}, v)$ with mean $\hat{f}$ and variance v,

$$\hat{f}(\bar{x}) = k^T C^{-1} y \text{ and } v(\bar{x}) = \kappa - k^T C^{-1} k. \tag{35}$$

This is a key result that defines GP regression. The mean function $\hat{f}(x)$ of the GP provides a prediction of the objective function $f(x)$. Furthermore, the variance function $v(x)$ can be used to measure the uncertainty level of the predictions with the mean value $\hat{f}$. The learning is shown numerically in the simulation section IX.

A. Learning in Auctions with Malicious Users

GP regression learning is used now to learn the utilities by malicious users in auctions. The first order condition for best response of malicious user from equation (5) gives

$$\frac{\partial J_i^m}{\partial x_i} = 0 \Rightarrow c_i' - U_i' - \theta_i \sum_{j \neq i} \frac{\partial U_j}{\partial Q_j} \frac{\partial Q_j}{\partial x_i} = 0.$$

We could see that the malicious user requires the marginal utility of all selfish users, i.e., $\frac{\partial U_j}{\partial Q_j} \forall j \neq i$ for calculating the best response. But for selfish users

$$c_j' - \frac{\partial U_j}{\partial Q_j} \frac{\partial Q_j}{\partial x_j} = 0, \ \ \forall j.$$

Therefore, by observing the best response bid, the marginal utilities of selfish users can be obtained by malicious users since the allocation and pricing are common knowledge.

To illustrate the approach, consider the case of logarithmic utility function weighted by a positive scalar parameter α, i.e.,

$$U_i = \alpha_i \log Q_i \ \ \forall i \in \mathcal{A}.$$

The best response for selfish users is $x_i^* = \alpha_i$. The unknown α's are then learned in single iteration from the bid.

Consider next the alternative case of exponential user utilities,

$$U_i = 1 - e^{-\alpha_i Q_i} \ \ \forall i \in \mathcal{A}.$$

In this case $x_i^* = \frac{S_i}{C\alpha_i} \log \frac{S_i}{C\alpha_i}$. So to learn α's using the bids, a single iteration is needed and the malicious user can calculate the best response in next iterations based on the bids of selfish users.

In the case of general user utilities, however, multiple steps of the regression algorithm are required in order for the malicious user to characterize the selfish user utilities with sufficient accuracy.

B. Learning in Pricing Mechanisms with Malicious Users

In this section, regression techniques are used to learn the user private utilities by the malicious user for implementation of pricing mechanisms. The best response equation for the malicious user is

$$P_i - U_i'(x_i) - \theta_i \sum_{j \in \mathcal{S}} \frac{\partial U_j(x_j(x_{-j}))}{\partial x_i} = 0.$$

The malicious user requires the shape of marginal utility of all selfish users, i.e., $\dfrac{\partial U_j}{\partial x_j} \forall j \neq i$ for calculating the best response. The malicious user observes the prices for M slots $\{P_1, \cdots, P_M\}$ set by the social planner which is same for every user and the response by each selfish user i which contains bid vector $\{x_{i1}, \cdots, x_{iM}\}\ \forall i$. Let the corresponding scalar marginal utility values at those points $U_i'(x_{i1}, \cdots, U_i'(x_{iM})\ \forall i$ which are equal to the prices. Assume that the observations are distorted by a zero-mean Gaussian noise, n with variance $\sigma \sim \mathcal{N}(0, \sigma)$. Now let the Gaussian vector obtained is, $\{y_{i1}, \cdots, y_{iM}\}\ \forall i$ where

$$y_{im} = U_i'(x_{im}) + n_i \ \forall i.$$

These data points can be used for the online learning of the marginal utilities by the malicious user. The algorithm of learning is given below.

Algorithm 1: Regression Learning of User utilities in Pricing Mechanisms by Malicious Users

Input: *Designer*: Global objective.
Input: *Regular Users*: Utility functions $U_i(x_i)$
Input: *Malicious User*: Utility functions $U_i^m(x_i)$
Result: Learned utility functions $\tilde{U_i}(x)\ \forall i$, optimal prices, and efficient allocation vector x^*

repeat
  begin *Designer:*
    Update the value of λ using $\lambda_{n+1} = \lambda_n + \kappa_D\big(\sum_i x_i - C\big)$;
    Using $\tilde{U_i}$, find the corresponding values of x;
    Continue until $\sum_i x_i = C$ **and denote the corresponding** λ_n **as** λ_{new};
    Set λ_{new} **as the user prices,** P_i ;
    begin *Regular Users:*
      foreach *Regular Users* i **do**
        Take action x_{inew} as response to the prices P_i;
      end
    end
    Malicious User: Observe the player actions $x_{inew}\ \forall i, m$;
    Add the values of λ_{new} and x_{new} to the initial data set points;
    Update user utility estimates $\tilde{U_i}$ and variances v_i for all the users based on the updated data set using GP;
  end
until *convergence*;

A Gaussian regression technique as described above is used to estimate the marginal utility functions $\tilde{U_i'}$ of the selfish users from which the utility functions can be constructed. The simulation results showing the learning is given in the Section IX.

VIII. Response Mechanisms to Malicious Users

The robustness analyses in the previous sections only measure the effect of selfish and malicious users but does not provide a way to encounter them. In this section, we consider a possible response schemes to adversarial behavior, based on softer punishment scheme using differentiated pricing.

A. Differentiated Pricing

We consider a softer response scheme than blocking towards malicious users after explicit detection based on any well known (threshold) detection scheme. There are numerous methods of detection already available as given in PART IV of [40]. The response mechanism is implemented by the designer by deploying a differentiated pricing. First, we define a trade-off metric $T(M)$ for quantifying the vulnerability of a pricing-based response to a mechanism M. This metric provides a way to measure the trade-off between the damage due to malicious users and how much effort (price) it costs them to create this damage.

Definition VIII.1. *A metric for quantifying vulnerability of a pricing-based response mechanism against a set of malicious users $B \subset \mathcal{A}$ is defined as:*

$$T(M) \geq \frac{\sum_{j\in\mathcal{S}} U_j(Q'_j(x)) - \sum_{j\in\mathcal{S}} U_j(Q_j(x))}{\sum_{k\in\mathcal{B}} c_k(x)},$$

and the lower bound is achieved in the best case scenario of perfect differentiation in terms of pricing.

Now we utilize this metric to evaluate the properties of the differentiated pricing scheme on example networks. A necessary assumption we make in this subsection is that malicious users stay within the system and do not have any means to evade the pricing mechanisms imposed by the designer. This assumption is relaxed in the next subsection.

Auctions for Additive Sharing

We derive now a differentiated payment function to counter the malicious behavior of users. It is assumed here that the designer knows the value of θ of malicious user. In practical problems, this is not realistic and the designer needs to make the decision on payment function entirely based on user bids. Therefore, we assume that after detecting the malicious user using a threshold detection scheme based on the bids, the designer punishes the malicious users with a price function assuming $\theta = -1$, i.e, extreme maliciousness. Alternatively, once can couple this parameter with the confidence of the detection scheme used, i.e. low θ values for high probability of malicious behavior and vice versa. The best response of the i^{th} user who tries to minimize her cost in terms of the signal or bid to be sent is obtained by computing

$$\frac{\partial J_i}{\partial x_i} = \frac{\partial c_i}{\partial x_i} - \frac{\partial U_i}{\partial Q_i}\frac{\sum_{j\neq i} x_j}{(\sum_k x_k)^2} + \theta_i \sum_{j\neq i} \frac{\alpha_j}{x_j \sum_k x_k} = 0. \tag{36}$$

This condition is necessary and sufficient for optimality. Then,

$$\frac{\partial U_i(Q_i)}{\partial Q_i} = \frac{(\sum_k x_k)^2}{\sum_{j\neq i} x_j}\left(\frac{\partial c_i}{\partial x_i} + \theta_i \sum_{j\neq i} \frac{\alpha_j}{x_j \sum_k x_k}\right).$$

Let us denote $t = \sum_j x_j$, then $x_i = \dfrac{tQ_i}{C}$ and

$$\sum_{j\neq i} x_j = t - x_i = t\left(1 - \frac{Q_i}{C}\right).$$

Doing the substitutions,

$$\begin{aligned}\frac{\partial U_i(Q_i)}{\partial Q_i} &= \frac{t}{1-\dfrac{Q_i}{C}}\left(\frac{\partial c_i(Q_i,t)}{\partial x_i} + \theta_i \sum_{j\neq i}\frac{1}{t}\right) \\ &:= f(Q_i,t).\end{aligned} \tag{37}$$

When we compare (37) and (8), we can see that $f(Q_i,t)$ is equal to the Lagrange multiplier λ. Since $f(Q_i,t)$ is a function of Q_i, there will be unequal marginal valuations at equilibrium. For efficient allocation we need to obtain a price function which will induce a $f(Q_i,t)$ which will give identical marginal valuations at equilibrium [18]. For this we make $f(Q_i,t)$ independent of Q_i and derive corresponding price function. Let $f(Q_i,t) = g(t)$ where $g(t)$ is the generator function and

$$\frac{\partial c_i}{\partial x_i} = \frac{\sum_{j\neq i} x_j g(t)}{(\sum_k x_k)^2} - \theta_i \frac{1}{\sum_k x_k}\sum_{j\neq i}\frac{\alpha_j}{x_j}.$$

By integrating over x_i, we obtain

$$\begin{aligned} c_i(x) &= \int_0^{x_i} \frac{g(s+\sum_{j\neq i} x_j)}{(s+\sum_{j\neq i} x_j)^2} ds \sum_{j\neq i} x_j \\ &- \theta_i \int_0^{x_i} \frac{ds}{s+\sum_{k\neq j} x_k} \sum_{j\neq i} \frac{\alpha_j}{x_j}. \end{aligned} \tag{38}$$

For $g(t) = t^3$, we obtain

$$\begin{aligned} c_i(x) &= \frac{\sum_{j\neq i} x_j}{2}((\sum_j x_j)^2 - (\sum_{j\neq i} x_j)^2) \\ &- \theta_i \log(1+\frac{x_i}{\sum_{j\neq i} x_j}) \sum_{j\neq i} \frac{\alpha_j}{x_j}. \end{aligned} \tag{39}$$

Let us assume that the users except i^{th} user are merely selfish due to the payment function of the mechanism they report $x_i = \alpha_i$. If the designer punishes the users who are detected as malicious with a payment in which $\theta_i = -1$, then the final pricing function becomes

$$c_i(x) = x_i \sum_{j\neq i} x_j + \log(1+\frac{x_i}{\sum_{j\neq i} x_j})(N-1). \tag{40}$$

For this cost function to be convex

$$N \leq \frac{\sum_{j\neq i} x_j (\sum_j x_j)^2}{2} + 1.$$

Now we can define a mechanism M_m which is defined by the allocation rule given in (10) and pricing rule given by (40) for malicious user and by (11) for regular user. Note that in this differentiated pricing scheme, the malicious users who will try to bid something higher than its private value will have to pay an additional amount proportional to their bid. Also, the payment by the malicious user is not convex. But this does not affect the equilibrium since anticipating the additional payment the malicious user will bid taking the best response according to the cost with payment given by equation (11) which is convex.

The tradeoff-parameter of mechanism M_m is given by,

$$T(M_m) \geq \frac{\sum_{j\in\mathcal{S}} \alpha_j \log(r_j)}{\sum_{i\in\mathcal{B}} x_i \sum_{j\neq i} x_j + \log(1+\frac{x_i}{\sum_{j\neq i} x_j})(N-1)}.$$

Such a differentiated pricing scheme is widely used today in various settings, such as network access. For example, if some users of an Internet Service Provider (ISP) are creating burden to the network by using much higher amount of resources above a pre-determined cap, they are priced differentially higher compared to other users. This reality is captured in our model since the higher usage above a threshold is punished even if it is not coming from the disproportionate use due to malicious nature.

In a similar way, a differentiated pricing mechanism can be also derived for interference coupled CDMA systems.

Pricing Mechanism for Additive Sharing

Let us consider the counterpart of pricing mechanism in additive sharing given in the previous section and study the effect of the differentiated pricing in that case. As one possibility we model the utility function of a malicious player as $U_i(x_i) = e^{\beta_i x_i}$, which reflects aggressive behavior in terms of resource demand. Note that this is still private information unknown to the designer. As a result, A malicious user takes a share of $x_m \in (\overline{x}+\epsilon, x_{max})$, where $\overline{x}$ is the mean and ϵ is some integer multiple of standard deviation of the demand vector x.

In order to counter the malicious behavior, the designer deploys differentiated pricing as part of a new mechanism M_e, which is a modified version of M_c. It is characterized by the pricing function

$$P_i^d = \begin{cases} f(\kappa_i(x_i - (\overline{x}+\epsilon))) & \text{for } x_i \geq b \\ P_i & \text{for } x_i \leq b \end{cases},$$

where b is determined by a statistical method, for example $b = \overline{x} + k\sigma_x$, where $\overline{x}$ is the mean and σ_x is standard deviation and P_i is the pricing function in the original mechanism. The function $f(.)$ is selected suitably depending on the utility functions of selfish and malicious users. If it is assumed that selfish users have continuous and differentiable concave utility function and malicious users have convex utility functions, then $f(.)$ can be a continuous and differentiable convex function. For the logarithmic utility function assumed here for selfish users, we take $f(.)$ as exponential function. The value of b can be

obtained alternatively from a clustering method or another Maximum-likelihood algorithm. Note that, the designer punishes the malicious players by employing a price function which increases exponentially with the share of resource taken by them, i.e. if they deviate too much from the mean behavior and create a significant burden on the system.

For the case of exponential pricing function, $T(M_e)$ is obtained as,

$$T(M_e) \geq \frac{\sum_{j\in\mathcal{S}} \alpha_j \log(\frac{C\lambda'}{\sum_i \alpha_i})}{\sum_{i\in\mathcal{B}} e^{\kappa_i(x_i-(\overline{x}+\epsilon))}}.$$

In the symmetric and only one malicious user case, it becomes

$$T(M_e) \geq \frac{\log(\frac{C\lambda'}{N\alpha})}{e^{\kappa_i(x_i-(\overline{x}+\epsilon))}}.$$

Pricing Mechanism for Interference Coupled Systems

Consider the case of pricing in interference coupled systems given in Section IV. To counter the malicious behavior, the designer introduces a new mechanism M_f which employs the differentiated pricing given by

$$P_i^d = \begin{cases} f(\kappa_i(\gamma_i(x_i, x_{-i}) - \gamma_i(\overline{x}+\epsilon, x_{-i}))) & \text{for } x_i \geq b \\ P_i & \text{for } x_i \leq b \end{cases},$$

In the case of logarithmic utility, $P_i = \lambda + \sum_{j\neq i} \frac{\alpha_j}{I_j}$, where λ is the Lagrange multiplier of the associated optimization problem and $I_i := \sum_{j\neq i} x_j + \sigma$ is the interference affecting player i [16], [17]. For the mechanism M_f, the trade-off metric $T(M_f)$ can be obtained in similar way as for additive sharing case. The variation of values of $T(M_e)$ and $T(M_f)$ for different number of users is given and compared with each other in the simulation section.

IX. Simulations

In this section, computer simulation results are presented to show the different parameters of the proposed mechanisms. First, the Price of Malice $PoM(M_a)$ and $PoM(M_b)$ of auction mechanism for additive sharing M_a and interference coupling M_b, respectively, using the setup in Section IV by varying the value of θ from -1 to 0. The number of users $N = 50$ out of which 10 users are taken to be malicious with same θ value. The other system parameters are $C = 30$ and $\sigma = 1$. The simulations are done by generating the player preferences α's according to a uniform distribution on the support set $[0, 10]$ and plotted in Figure 1. It can be observed that value of $PoM(M_a)$ and $PoM(M_b)$ decreases as θ varies from -1 to 0 as expected.

We next compute the Price of Malice $PoM(M_c)$ and $PoM(M_d)$ for the pricing mechanism for additive sharing M_c and interference coupling M_d, respectively, using the setup in Example 3 by varying the number of users from 8 to 15. The simulations are done by generating the player preferences α's according to a uniform distribution on the support set $[0, 2]$ and repeated 100 times. Then, the mean and standard deviation of the obtained $PoM(M)$ values are plotted in Figure 2. The number of malicious users is fixed at 3, $C = 5$, $\sigma = 0.5$ and $x_{max} = 1$. The malicious users take an allocation x_{max} and remaining share is allocated using respective iterative algorithms among good users. The quantities $PoM(M_c)$ and $PoM(M_d)$ are plotted in Figure 2. It can be observed that, for a fixed number of malicious users, as number of users increases the mechanisms become more robust, as expected.

Next the variation of value of ϵ for the ϵ-group strategyproof mechanism $\mathcal{M}_a$ is simulated. The variation of value of ϵ defined in (28) with number of malicious users for the mechanism $\mathcal{M}_a$ is plotted in Figure 3. The total number of users including the malicious users is fixed at 20. We can observe that the value of ϵ increases as the portion of malicious users increases, as expected.

Next, the trade-off parameter $T(M)$ is plotted for auction mechanism M_m for additive sharing for different values of θ in Figure 4. The users having $x > \overline{x} + 2\ \sigma_x$ are priced differentially as described in Section VIII.

Finally, the trade-off parameter $T(M)$ is plotted for pricing mechanisms M_e and M_f in Figure 5. An iterative algorithm as given in [17] is used to obtain allocation and prices. The other parameters remain the same as those used to generate the Figure 2. It can be seen from Figure 5 that mechanism M_f performs better than M_e in this case, possibly due to the coupling involved. In Figure 6, for the pricing case the actual marginal utility curves for 3 users with logarithmic utilities are compared with marginal utility curves constructed using initial data points and the online algorithm given in VII. We can observe that near the optimal lambda value the estimation of the function is better with the online algorithm than with only initial data points, as expected.

X. Conclusion

We have studied adversarial behavior in network resource allocation schemes including pricing and auctions by adopting a mechanism design approach to measure and counter it. First, we have analyzed the robustness of the existing network

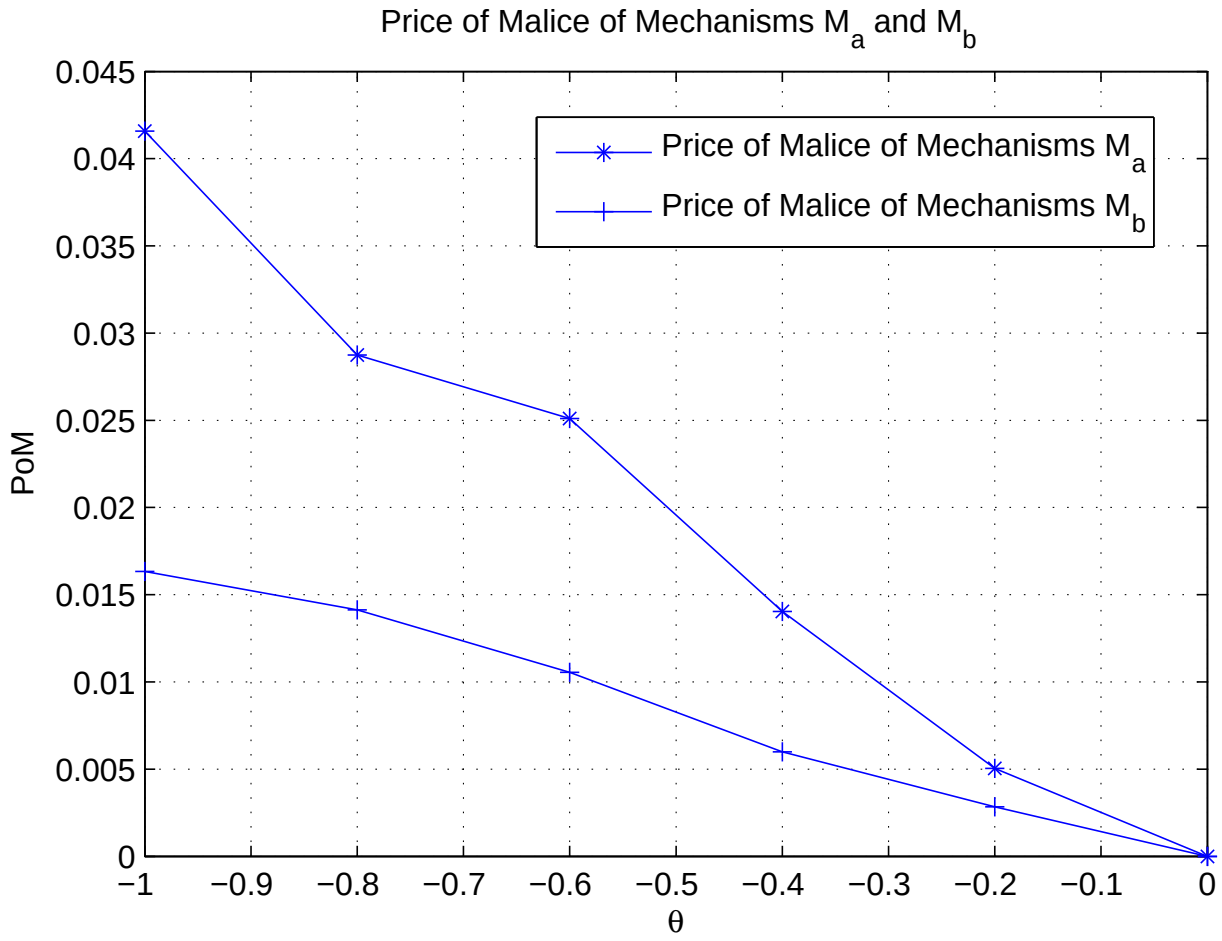


Fig. 1. Price of Malice $PoM(M)$ of the auction mechanism for additive coupling $\mathcal{M}_a$ and interference coupling $\mathcal{M}_b$ for varying values of θ.

mechanisms to adversarial behavior, which ranges from extreme selfishness to destructive maliciousness, using a quantitative metric Price of Malice. We have considered two types of coupling of resource sharing, additive and interference coupling. In the pricing case an iterative distributed algorithm is proposed and its convergence is analyzed. Next one of the mechanism is proved to be ϵ-group strategy-proof against the collusion behavior of malicious users. Then learning methods are used to estimate the marginal utilities of selfish users by the malicious user. In the simulation, we show that the functions can be approximated well by the Gaussian regression method. Next, we have presented one method to counter such adversarial behavior which is a differentiated pricing to punish the aggressive user. Finally, the results obtained have been illustrated with multiple examples and numerical simulations.

Future research directions include obtaining bounds on the parameters dealt in this paper and behavioral detection schemes. It is also an interesting direction to analyze the effect of altruism or partial altruism of some of the users in this context, as in the work [14].

REFERENCES

[1] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *MobiHoc '05 Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, 2005, pp. 47–56.

[2] K. Avrachenkov, E. Altman, and A. Garnaev, "A jamming game in wireless networks with transmission cost," *Lecture Notes in Computer Science*, vol. 4465, pp. 1–12, 2007.

[3] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, 2nd ed. Philadelphia, PA: SIAM, 1999.

[4] V. Krishna, *Auction Theory*. Amazon: Academic Press 1st edition, 2002.

[5] W. Vickrey, "Counterspeculation, auctions and competitive sealed tenders," *Journal of Finance*, vol. 16, no. 1, pp. 8–37, 1961.

[6] T. Moscibroda, S. Schmid, and R. Wattenhofer, "When selfish meets evil: byzantine players in a virus inoculation game," in *Proceedings of the twenty-fifth annual ACM symposium on Principles of distributed computing*, Denver, Colorado, 2006.

[7] M. Babaioff, R.Kleinberg, and C. H. Papadimitriou, "Congestion games with malicious players," in *Proceedings of the 8th ACM conference on Electronic commerce*, San Diego, California, 2007, pp. 103–112.

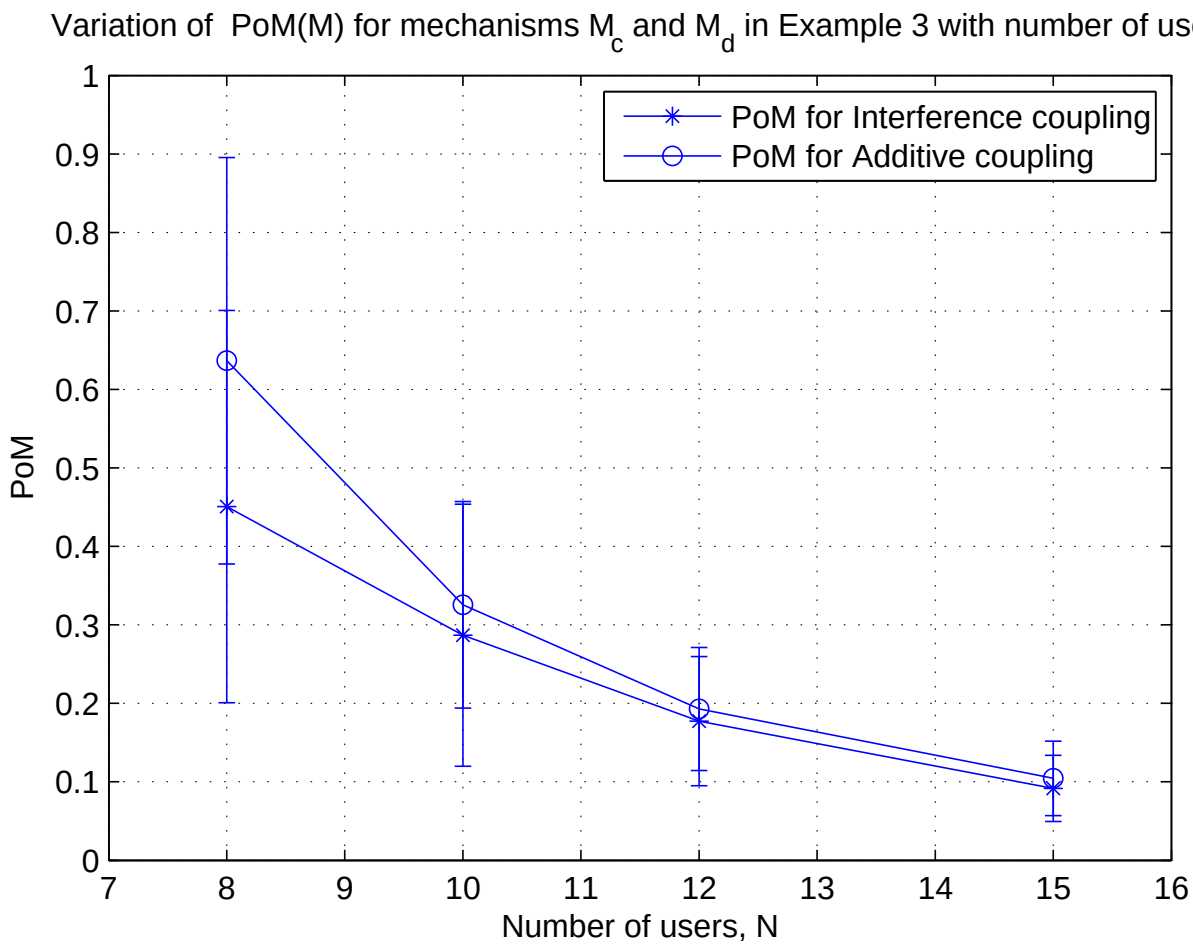


Fig. 2. Price of Malice $PoM(M)$ of the pricing mechanisms for additive coupling $\mathcal{M}_c$ and interference coupling $\mathcal{M}_d$ for varying number of users.

[8] A. K. Chorppath and T. Alpcan, "Learning user preferences in mechanism design," in *In Proc. of 50th IEEE Conference on Decision and Control and European Control Conference*, Orlando, Florida, December 2011.

[9] C. E. Rasmussen and C. K. I. Williams, *Gaussian Processes for Machine Learning (Adaptive Computation and Machine Learning)*. The MIT Press, 2005. [Online]. Available: http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20&path=ASIN/026218253X

[10] E. Koutsoupias and C. Papadimitriou, "Worst-case equilibria," *Lecture Notes in Computer Science*, pp. 404–413, 1999.

[11] T. Roughgarden, "The price of anarchy is independent of the network topology," in *Proceedings of the 34th Annual ACM Symposium on the Theory of Computing*, May 2002.

[12] A. Roth, "The price of malice in linear congestion games," in *In WINE '08: Proceedings of the 4th International Workshop on Internet and Network Economics*, 2008, pp. 118–125.

[13] S.Theodorakopoulos and J. S. Baras, "Game theoretic modeling of malicious users in collaborative networks," *IEEE Journal on selected areas in communications*, vol. 26, no. 7, pp. 1317–1327, August 2008.

[14] P. A. Chen and D. Kempe, "Altruism, selfishness, and spite in traffic routing," in *Electronic Commerce, EC08*, Chicago, Illinois, July 2008, pp. 8–125.

[15] F. P. Kelly, A. K. Maulloo, and D. Tan, "Rate control in communication networks: shadow prices, proportional fairness and stability," *Journal of the Operational Research Society*, vol. 49, pp. 237–252, 1998.

[16] T. Alpcan and L. Pavel, "Nash Equilibrium Design and Optimization," in *Proc. of Intl. Conf. on Game Theory for Networks (GameNets 2009)*, Istanbul, Turkey, May 2009.

[17] H. Boche, S. Naik, and T. Alpcan, "A unified mechanism design framework for networked systems," arXiv:1009.0377[cs.GT], Tech. Rep., September 2010. [Online]. Available: arxiv.org

[18] R. T. Maheswaran and T. Basar, "Social Welfare of Selfish Agents: Motivating Efficiency for Divisible Resources," in *43rd IEEE Conf. on Decision and Control (CDC)*, Paradise Island, Bahamas, December 2004, pp. 1550–1555.

[19] R. Johari, S. Mannor, and J. Tsitsiklis, "Efficiency loss in a network resource allocation game: the case of elastic supply," *IEEE Transactions on Automatic Control*, vol. 50, no. 11, pp. 1712–1724, November 2005.

[20] F. Brandt, T. Sandholm, and Y. Shoham, "Spiteful bidding in sealed-bid auctions," in *IJCAI'07 Proceedings of the 20th international joint conference on Artifical Intelligence*, Hyderabad, India, 2007, pp. 1207–1214.

[21] A. P. Azad, E. Altman, and R. E. Azouzi, "From altruism to non-cooperation in routing games," *CoRR*, vol. abs/0808.4079, 2008.

[22] A. P. Azad and J. Musacchio, "Unilateral altruism in network routing games with atomic players," *CoRR*, vol. abs/1108.1233, 2011.

[23] H.Moulin and S.Shenker, "Strategyproof sharing of submodular costs: budget balance versus efficiency," *Journal on economic theory*, vol. 18, no. 3, pp. 511–533, August 2001.

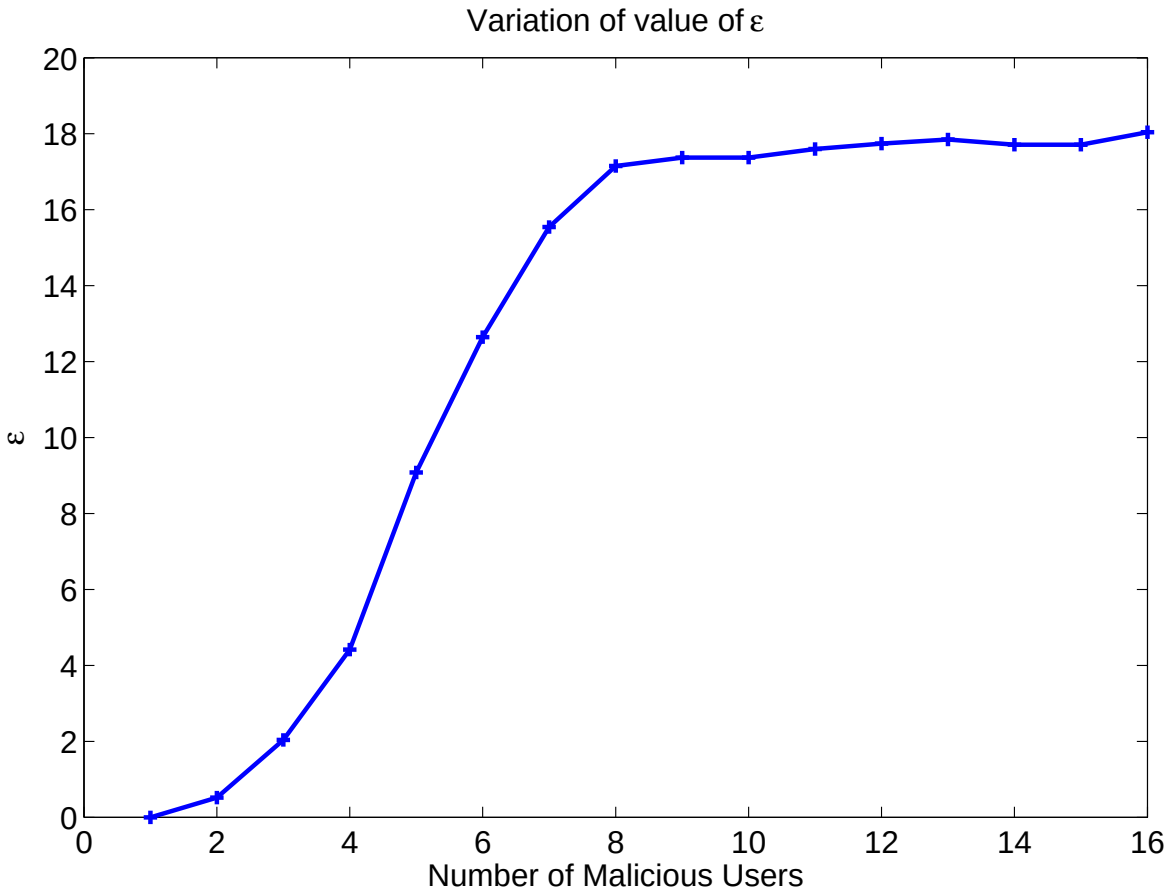


Fig. 3. Variation of value of ϵ with number of malicious users for the ϵ-group strategyproof mechanism $\mathcal{M}_a$.

[24] J. Brenner and G. Schafer, "Group-strategyproof cost sharing mechanisms for makespan and other scheduling problems," *Theoretical Computer Science*, vol. 401, no. 3, pp. 96–106, 2008.

[25] A. Hayrapetyan, E. Tardos, and T. Wexler, "The effect of collusion in congestion games," in *Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, ser. STOC '06. New York, NY, USA: ACM, 2006, pp. 89–98. [Online]. Available: http://doi.acm.org/10.1145/1132516.1132529

[26] E. Altman, H. Kameda, and Y. Hayel, "Revisiting collusion in routing games: A load balancing problem," in *Network Games, Control and Optimization (NetGCooP), 2011 5th International Conference on*, oct. 2011, pp. 1 –6.

[27] J. C. HARSANYI, "Games with incomplete information played by 'bayesian' players," *Management Science, Theory Series*, vol. 14, no. 3, 1967.

[28] R. J. Aumann, "Correlated equilibrium as an expression of bayesian rationality," *Econometrica*, vol. 55, no. 1, pp. 1 – 18, 1987.

[29] M.-F. Balcan, A. Blum, J. D. Hartline, and Y. Mansour, "Reducing mechanism design to algorithm design via machine learning," *J. Comput. Syst. Sci.*, vol. 74, pp. 1245–1270, December 2008. [Online]. Available: http://portal.acm.org/citation.cfm?id=1460945.1461324

[30] S. Micali and P. Valiant, "Revenue in truly combinatorial auctions and adversarial mechanism design," MIT-Computer Science and Artificial Intelligence Laboratory, Tech. Rep., June 2008. [Online]. Available: http://dspace.mit.edu/handle/1721.1/41872

[31] V. Krishna, *Auction theory (2nd ed.)*. Academic Press, 2010.

[32] R. Srikant, *The Mathematics of Internet Congestion Control*, ser. Systems & Control: Foundations & Applications. Boston, MA: Birkhauser, 2004.

[33] T. Alpcan and T. Başar, "A Utility-Based Congestion Control Scheme for Internet-Style Networks with Delay," *IEEE Trans. on Networking*, vol. 13, no. 6, pp. 1261–1274, December 2005.

[34] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n -person games," *Econometrica*, vol. 33, no. 3, pp. 520–534, 1965.

[35] J. Huang, R. Berry, and M. Honig, "Auction–based Spectrum Sharing," *ACM Mobile Networks and Applications Journal*, vol. 24, no. 5, pp. 405–418, June 2006.

[36] A. K. Chorppath, S. Bhashyam, and R. Sundaresan, "A convex optimization framework for almost budget balanced allocation of a divisible good," *IEEE Transactions on Automation Science and Engineering*, 2011.

[37] A. K. Chorppath, T. Alpcan, and H. Boche, "Pricing mechanisms for multi-carrier wireless systems," in *in Proc. of IEEE Intl. Dynamic Spectrum Access Networks (DySPAN) Symp.*, Aachen, Germany, May 2011.

[38] K. S. J. Morgan and G. Reis, "The spite motive and equilibrium behavior in auctions," *Contributions to Economic Analysis and Policy*, vol. 2, no. 5, 2003.

[39] D. P. Bertsekas and J. Tsitsiklis, *Parallel and Distributed Computation: Numerical Methods*, 1st ed. Athena Scientific, 1997.

[40] T. Alpcan and T. Basar, *Network Security: A Decision and Game Theoretic Approach*. Cambridge, U.K, Cambridge Univ. Press, 2010.

XI. APPENDIX

Definitions:

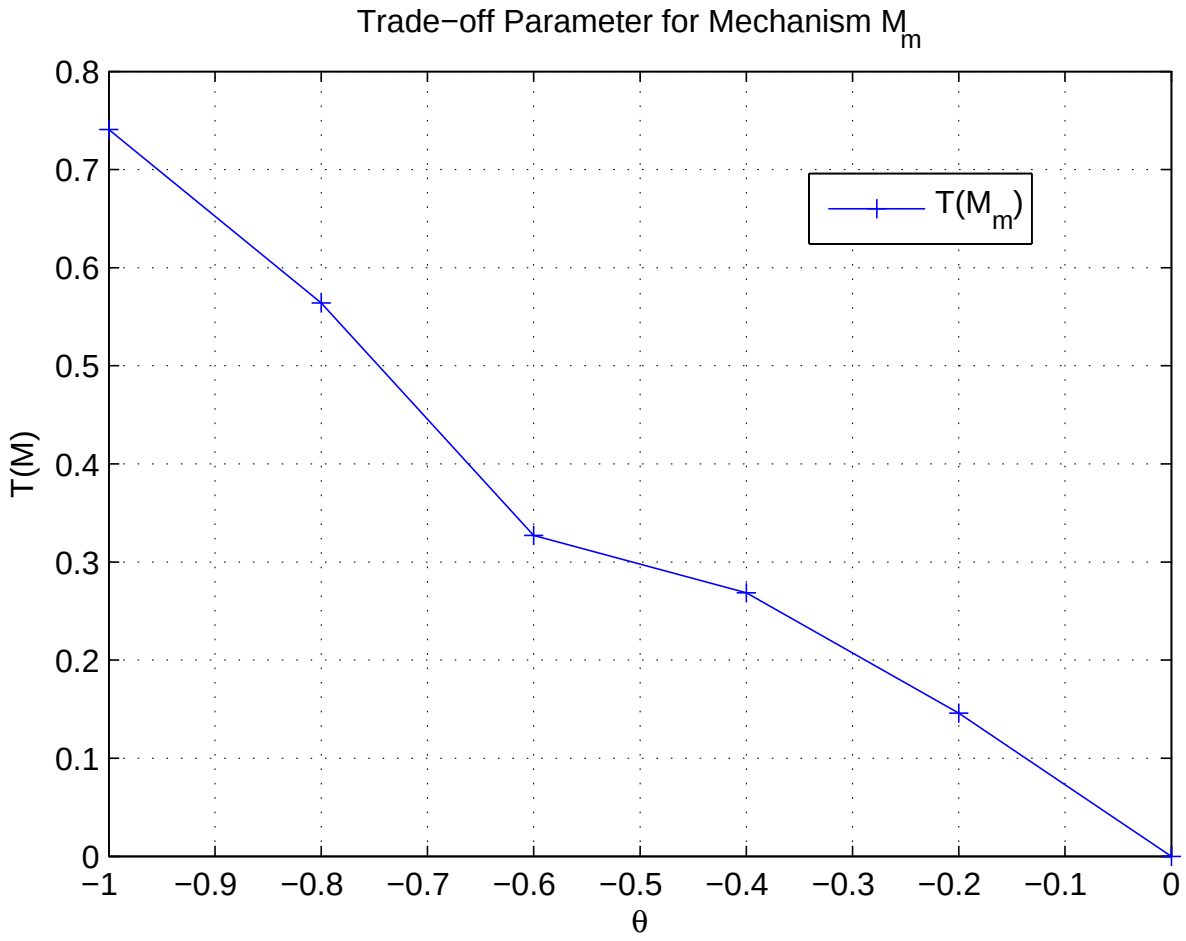


Fig. 4. Trade off parameter $T(M)$ of auction mechanism M_m for additive sharing for varying values of θ.

The properties of mechanisms considered in this paper can be formally defined as follows.

Definition 5. **Efficiency:** Efficient mechanisms maximize designer objective, i.e. they solve the problem $\max_x V(x, U_i(x), c_i(x))$.

Definition 6. **Nash Equilibrium:** The strategy profile $x^* = [x_1^*, \ldots, x_N^*]$ is in Nash Equilibrium if the cost of each player is minimized at the equilibrium given the best strategies of other players.

$$J_i(x_i^*, x_{-i}^*) \leq J_i(x_i, x_{-i}^*), \forall i \in \mathcal{A}, x_i \in \mathcal{X}_i$$

Definition 7. **Dominant Strategy Equilibrium:** The strategy profile $\tilde{x} = [\tilde{x}_1, \ldots, \tilde{x}_N]$ is in Dominant Strategy Equilibrium if the cost of each player is minimized at the equilibrium irrespective of the strategies of other players.

$$J_i(\tilde{x_i}, x_{-i}) \leq J_i(x_i, x_{-i}), \forall i \in \mathcal{A}, x_i \in \mathcal{X}_i, x_{-i} \in \mathcal{X}_{-i}$$

Definition 8. **Strategy-proofness or Dominant Strategy Incentive Compatibility:** If the players do not gain anything by reporting a value other than their true value in the dominant strategy equilibrium, i.e.

$$J_i(x_i^t, x_{-i}) \leq J_i(x_i', x_{-i}), \forall i \in \mathcal{A}, x_i \in \mathcal{X}_i, x_{-i} \in \mathcal{X}_{-i}$$

where x^t is the original value vector, and x' is the "misrepresented" value or action, then the mechanism is strategy-proof.

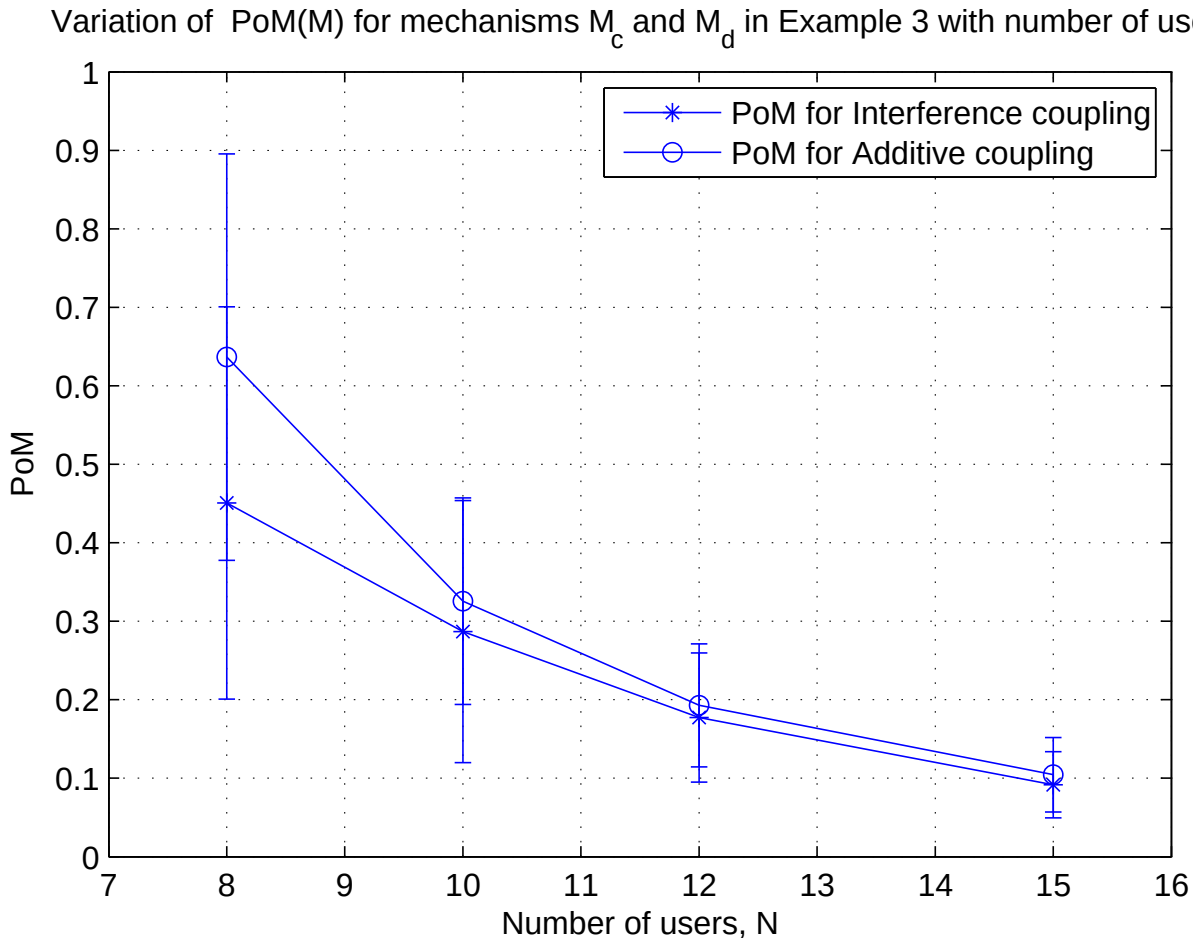


Fig. 5. Trade off parameter $T(M)$ of pricing mechanisms for additive coupling $\mathcal{M}_e$ and interference coupling $\mathcal{M}_f$ in Examples 3 and 4 respectively with varying number of users.

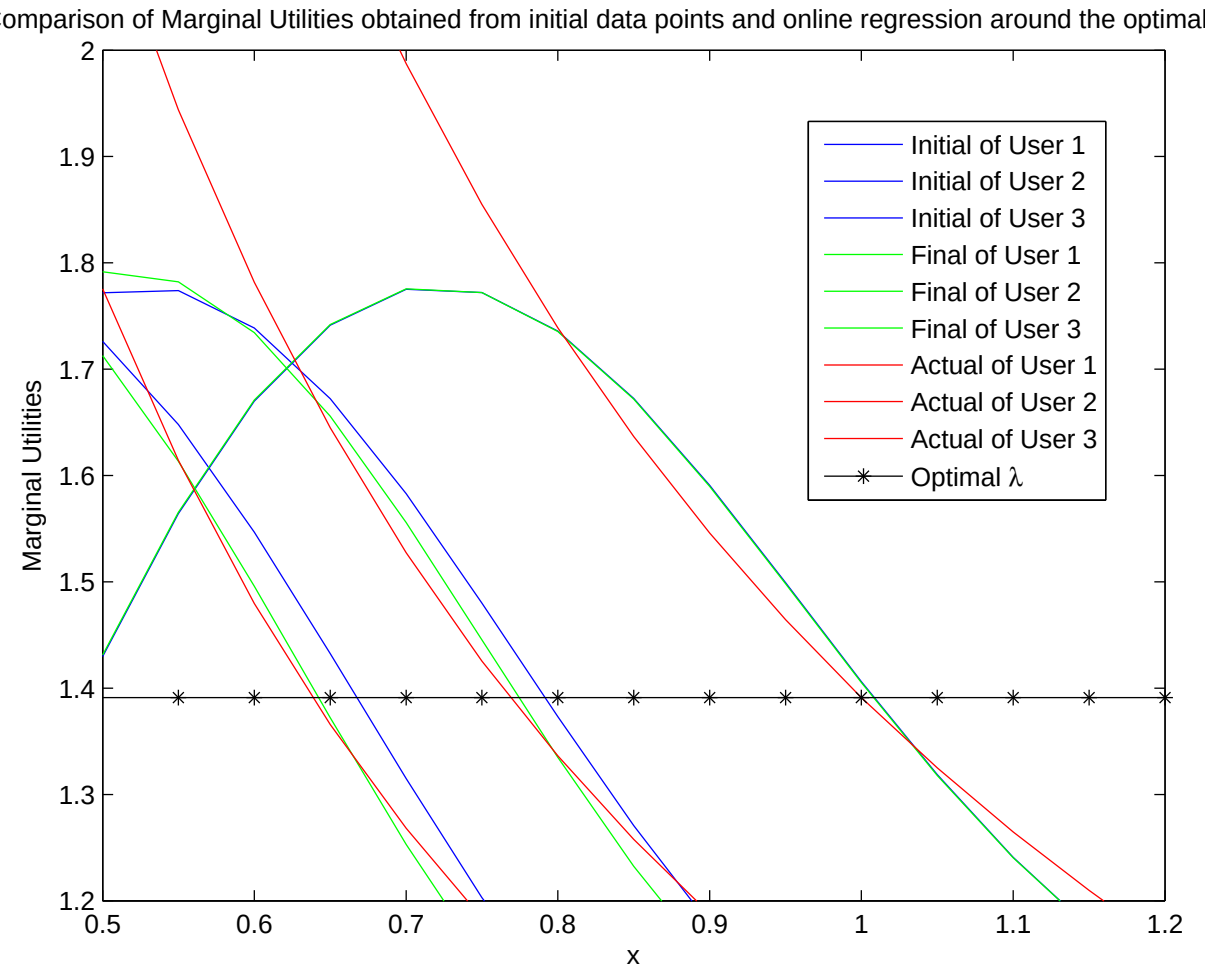


Fig. 6. Marginal Utility curve for logarithmic utilities constructed using initial data points and the learning method given in VII.