Technische Universität München
Lehrstuhl für Theoretische Informationstechnik

Resource Allocation and Pricing Mechanisms for Wireless Networks with Malicious Users

Anil Kumar Chorppath

Vollständiger Abdruck der von der Fakultät für Elektrotechnik und Informationstechnik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktor- Ingenieurs

genehmigten Dissertation.

Vorsitzender: Univ.-Prof. Dr.-Ing. Wolfgang Kellerer
Prüfer der Dissertation:
1. Univ.-Prof. Dr.-Ing. Dr. rer. nat. Holger Boche
2. Prof. Tansu Alpcan, PhD., The University of Melbourne, Australien.

Die Dissertation wurde am 11.11.2014 bei der Technischen Universität München eingereicht und durch die Fakultät für Elektrotechnik und Informationstechnik am 10.07.2015 angenommen.

Resource Allocation and Pricing Mechanisms for Wireless Networks with Malicious Users

Anil Kumar Chorppath

Acknowledgment

First, I would like to thank my supervisors Dr. Tansu Alpcan and Prof. Holger Boche for giving the opportunity to work with them and for their great support throughout my PhD. I thank Dr. Tansu Alpcan who has acted as my mentor and provided valuable insights in all my works. I am also thankful to him for hosting me in The University of Melbourne, Australia and for finding time for late hour skype calls. I thank Prof. Holger Boche for the valuable suggestions and for showing the value of scientific rigor. I am also thankful to him for taking me with his group while moving from Berlin to Munich. I would like to thank Prof. Eduard Jorswieck, Prof. Edmund M. Yeh and Prof. Iordanis Koutsopoulos, for working with me in different projects. I thank George Iosifidis and Fei Shen for having nice discussions and co-writing papers with me. With George I also had the opportunity to discuss about many other things and to visit him in Athens.

I thank my colleagues in the chair, working with them was a nice experience. Philipp deserves a special mention for being my office-mate and for the grill and DJ sessions.

I would like to thank Prof. Srikrishna Bhashyam and Prof. Rajesh Sundaresan, who were my advisers during Master Thesis. They instilled in me the courage and the wish to do a PhD.

I would like to thank Telekom Innovation Laboratories, Berlin and the COIN project by German National Science Foundation (DFG) for financially supporting my work in this dissertation.

My friends Arvind, Martin, Lukas and Blanca were with me during the great times in the amazing city of Berlin. I am lucky having friends like Bejoy, Deniz(Charlie), Thaseem, Cyril, Milan, Arun, Rahul, Adithya, Omkar, Binoy, Babu, Adriana, Federico, Jean, Rahul Devassy and Victor. They drank with me and encouraged me to look at PhD in a relaxed way.

My friends, Padmanabhan, Rajet, Prashanth, Geordie, Dileep and Vinod, who were former employees of The Centre of Excellence in Wireless Technology (CEWiT), India, made me believe that PhD is a natural step after Masters.

I would like to acknowledge my Amma, Lakshmikutty Karonnanveettil and Achan, Ramankuttty Chorppath, for their encouragement to learn and for showing the value of persistence.

And, it was Sruthi who gave me strength throughout the final days of PhD.

Zusammenfassung

In dieser Dissertation, schlagen wir einen Rahmen für die Gestaltung von dezentralen Preismechanismen und zentralisierten Auktionsmechanismen ohne und mit böswilligen Benutzern vor. Zunächst entwerfen wir Preismechanismen für eine effiziente Leistungszuteilung in einem Uplink von Multi Carrier Code Division Multiple Access (MC-CDMA) mit price taking Nutzern. Der Mechanismus wird um Leistungsrestriktion auf die Nutzer sowie Träger und für die Umsatzmaximierung und Energieminimierung erweitert. Auch Preismechanismen werden für multihop heterogene drahtlose Netzwerke ausgelegt. Ein iterativer Algorithmus vorgeschlagen und seine Konvergenz bewiesen. Eine Regressions learning methode wird durch den Designer verwendet, um die Utility-Funktionen von Nutzern, von ihren Aktionen zu lernen. Wir verwenden diesen Preismechanismenrahmen, um einen Speicherort Privatsphrenmechanismus für Mobile Commerce mit Entropienutzenfunktionen und Budgetrestriktion zu entwerfen. Als nächstes wird ein zentralisierter Auktionsmechanismus mit price anticipating Nutzern vorgeschlagen und seine Effizienz nachgewiesen. Eine neue Modellierung für Nutzenfunktion von böswilligen Nutzern wird vorgeschlagen und eine Metrik Price of Malice (PoM) zur Quantifizierung der Wirkung der böswilligen Nutzern definiert. PoM für die Preismechanismen und die Auktionsmechanismen werden erhalten. Sowohl die Preismechanismen und Auktionsmechanismen werden modifiziert für die Anfechtung von böswilligen Nutzern. Weiter schwachen wir die Annahme, dass die Nutzer und der Designer wissen, die Art von Nutzern. Dann schlagen wir Bayes-Mechanismen. Die Bedingungen sind erhalten, unter denen die Unsicherheit über die Art der Nutzer ist Vorteil für die regelmigen Nutzer und Designer. Die Wahrscheinlichkeit, dass ein Nutzer böswillig ist, mit machine learning methoden aufgebaut. Die differenzierte Preis mit diese probabilistische Informationen wird implementiert. Dann Preismechanismen mit böswilligen Nutzer auf einen Fall, wo jeder Nutzer eine Quality of Service(QoS) Anforderung, erweitert.

Abstract

In this thesis, we propose a framework for designing decentralized pricing and centralized auction mechanisms in the presence and absence of malicious users. First, we design pricing mechanism for efficient power allocation in the uplink of a single cell Multi Carrier Code Division Multiple Access (MC-CDMA) system with strategic and price taking users. The mechanism is extended to sum power constraint over the users and carriers. Additionally, prices are designed for different designer objectives such as revenue maximization and energy minimization. We also consider multihop heterogeneous wireless networks and design appropriate pricing mechanisms for efficient joint power and rate allocation. An iterative algorithm for pricing mechanism is proposed and its convergence is proven. We use the pricing mechanism framework to design a location privacy mechanism for mobile commerce with entropy utility functions and a budget constraint. A regression learning method is used by the designer to learn the utility functions of users from their actions. This is in contrast to direct mechanisms where the designer asks the users to report their utility functions. Next, a centralized auction mechanism for networks with interference coupled utilities and price anticipating users is proposed and its efficiency is proven. A new modeling of malicious user utility function is proposed and a metric Price of Malice (PoM) for quantifying the effect of malicious users is defined. The PoM and related metrics for pricing and auction mechanisms are obtained. Then both the pricing and auction mechanisms are extended for countering the malicious users using differentiated pricing. Next, we relax the assumption that the users and the designer know the nature of users and design Bayesian mechanisms. By comparing to the complete information case, the conditions under which the uncertainty about the nature of the users is beneficial for the regular users and the designer, are obtained. The probability of a user being malicious is constructed using learning methods and the differentiated pricing is implemented using this probabilistic information. Then pricing mechanisms with malicious users are extended to a case where each user submits a Quality of Service(QoS) requirement.

History shows that where ethics and economics come in conflict, victory is always with economics. Vested interests have never been known to have willingly divested themselves unless there was sufficient force to compel them.

- Dr. Bhimrao Ramji Ambedkar, *The principal architect of the Constitution of India*, 1945.

Contents

List of Figures

List of Tables

1 Introduction

As mobile devices get higher computational and storage capability, the assumption that they will blindly follow the algorithms in the network does not hold anymore. When mobiles play a more active role in strategic resource allocation decisions in wireless networks, the interaction between the individual devices and system owners become more complex. The algorithms in the mobile devices will act strategically to gain better throughput to the devices at the expense of overall network performance. Also, the wireless users have the opportunity of manipulating the network by misrepresenting their private information for their own benefit. Some devices may even get better benefit from harming the throughput of other devices (users) by maliciously influencing the resource allocation algorithms. Therefore, the behavior of the users in a wireless network vary from selfish to extreme maliciousness. It is in the interest of the network to efficiently allocate scarce network resources such as power and spectrum to devices of competing interests in a decentralized network. For this, the network designs prices to align the utility of the individual devices to the network goal.

In this thesis, we propose a framework for designing decentralized pricing without and with malicious users. We address a class of problems known as *distributed mechanism design*, which deals with designing pricing for distributed networks. The designer (network) aims to design appropriate incentives and algorithms in order to achieve certain network level goals while additionally eliciting true preferences from users. We also propose centralized auction mechanisms where the designer has more control over the resource allocation. Mechanisms such as pricing schemes and auctions are utilized to design wireless resource allocation schemes, which can be analyzed within the mathematical framework of strategic (noncooperative) games. Although the participating players are selfish or malicious, these mechanisms ensure that the game outcome is optimal with respect to a global criterion (e.g. maximizing a social welfare function) and strategy-proof, i.e. players have no reason to deceive the designer. The mechanism designer achieves these objectives by introducing specific rules and incentives to the players; in this case, by adding resource prices to their utilities.

In this chapter, we provide the motivation behind the different problems addressed in this thesis, explain the previous results and give the contributions and the outline of the dissertation.

1.1 Power Control in Wireless Networks

In a distributed wireless network, the control of power allocation by the users is an important problem. The Signal-to-Interference plus Noise Ratio (SINR) based utilities received by the users bring interference coupled functions in the optimization problems

of the individual users and also base station. The strategic and selfish nature of the users in distributed wireless networks, makes game theory the most appropriate tool for analyzing the power allocation problems.

Price of Anarchy (PoA), first defined by E. Koutsoupias and C. Papadimitriou [71], can be summarized as loss in overall efficiency which occurs in networks when the users are selfish. It is a metric which quantify the efficiency loss in competition compared to cooperation. Distributed mechanism design aims to mitigate PoA and achieve system level goals such as maximization of aggregate user performance in the network.The network designs appropriate pricing for different network level goals based on the received SINR from all the users which is measured by the base station.

Next generation wireless systems for broadband wireless access allocate the frequency band simultaneously for multiple users over multiple orthogonal carriers using schemes such as Orthogonal Frequency Division Multiplexing Access(OFDMA), Orthogonal Frequency and Code Division Multiplexing (OFCDM) or Multi-Carrier Code Division Multiple Access (MC-CDMA)[107]. For instance, OFDMA is used in the downlink and Single Carrier FDMA (SC-FDMA) is used in the uplink of the 3GPP LTE standard. OFDMA results from combining Orthogonal Frequency Division Multiplexing (OFDM), which splits input stream of symbols into a number of parallel streams which are transmitted over orthogonal subcarriers, with Frequency Division Multiplexing Access (FDMA) technique [83]. OFDM has high robustness against multipath interference (MPI) as channel equalization can easily be performed in the frequency domain. OFDMA allows multiuser communication by dividing the available subcarriers to subchannels that are allocated to distinct users for simultaneous transmission.

Single-carrier CDMA is not suitable for communication over a broadband channel due to the vulnerability to multipath interference. Combining CDMA with OFDM as in MC-CDMA, benefits from the robustness of OFDM to MPI[78]. MC-CDMA also gives frequency diversity and facilitate one-cell frequency reuse in a cellular environment, in addition to the benefit of OFDM. Therefore, MC-CDMA is considered as a potential candidate for next generation broadband wireless systems. In MC-CDMA, the power strategy selected by one user affects other users through multiple access interference and this makes the game interactions between the users interesting.

In the first part of the thesis, we propose a framework to find the optimal pricing for a general multiuser multi-carrier wireless system. The optimal pricing function depends on the different network goals such as net utility maximization, revenue maximization and energy minimization. Another important factor is the topology of the network.

Due to their ability to bring about massive spatial reuse of frequency, small cell base stations such as Femto Base Stations (FBS) or Pico Base Stations (PBS) are increasingly important for improving network capacity. At the same time, FBSs also give better data rate to end users due to short transmission range and fewer users per cell. FBSs are normally deployed in indoor home or office environments owned or rented by second parties other than the service provider, and are normally underutilized. One way to better utilize the capacities of FBSs is to employ the FBSs as relays [43]. In this scenario, FBSs carry traffic from the Macro Base Station (MBS) to Macro Users (MUs), in addition to serving Femto Users (FUs). The relaying generates revenue for the owner of the

FBSs. Moreover, the relaying extends the coverage of FBSs to outdoor environments [51], thereby reducing the burden on the MBS. If the network is multihop, the pricing function need to take into account the power and rate allocation at different parts of the network. This thesis deals with designing prices for different network goals and also for multihop wireless networks.

1.2 Location Privacy and Security Problems in Wireless Networks

In mobile commerce, a company provides location based services to a set of mobile users who are concerned about their location privacy. The users report to the company their location with a level of granularity to maintain a degree of anonymity, depending on their perceived risk. According to the level of accuracy of information, the users receive in return monetary benefits or better services from the company. We formulate a quantitative model, in which information theoretic metrics such as entropy quantify the anonymity level of the users. The individual perceived risks of users and the benefits they obtain are considered to be linear functions of their chosen location information granularity. The interaction between the mobile commerce company and its users are investigated using mechanism design techniques as a privacy game. The user best responses and optimal strategies for the company are derived under budgetary constraints on incentives, which are provided to users in order to convince them to share their private information at the desired level of granularity.

Security problems in wireless networks include jamming, Denial of Service (DoS) attacks and Botnets. We propose a general framework to deal with these security problems and additionally address the specifics of jamming and Botnet problems. Botnets are software programs which compromise the networked devices (bots) and carry out Distributed Denial of Service (DDoS) attacks in the network. DDoS attacks use the overall network bandwidth and other resources of the bots, to deny the legitimate access to resources. The high inter-connectivity of the wireless network with the Internet makes these networks highly vulnerable to security attacks.There is a need for a different modeling of utility functions of malicious users who create security problems than the utility functions of regular users. This different modeling is important to find the resource allocation solutions and to quantify the effect of malicious users on the network performance. Also some of the malicious users collude to increase the impact of their activities on the regular users and to have selfish benefits. In the mechanism design literature, the mechanisms which are resistant to collusion are referred to as group-strategy proof mechanisms. The pricing schemes are vulnerable when there are malicious users in the network. In this dissertation, we quantify the effect of malicious users on the pricing schemes which are originally designed for networks with only selfish users. Then we modify these mechanisms to counter the malicious users.

Price of Malice (PoM) is a form of PoA which occurs in the presence of malicious users in the network. It quantifies the effect of malicious users on the net utilities of the regular users. The mechanism rules need to be modified to reduce the PoM. Mitigating

PoM is compelling than mitigating PoA, due to the difficulty in detecting the malicious users or obtaining the statistics about malicious user population int he network.

1.3 Wireless Networks with Limited Information

For the efficient resource allocation to the users, the designer need to know their utility functions which are usually infinite dimensional. In distributed mechanism design, the designer finds allocation and pricing rules based on the one dimensional scalar signals from the users. Alternatively, the designer can assume a surrogate utility function for the users and make them report a scalar parameter of the utility function [65]. Learning schemes can be used to obtain utility functions from the signals of the users for designing prices and allocation.

In realistic situations, the users are uncertain about the nature of other users, i.e. whether others are regular users or bots (malicious users). In this thesis, we study the conditions under which uncertainty in the network is beneficial for regular users. The boundary conditions are based on wireless system parameters. A malicious user does not want to harm other malicious users by unnecessarily spending more energy and paying more price for the extra power. Therefore, by creating the uncertainty about their nature by hiding, the regular users confuse the malicious users. The uncertainty created in the network is a way for the regular users to counter the malicious users and have better utility for themselves. By observing the network over long period of time, the designer forms probability distributions on the nature of users and then design prices based on them.

For different resource allocation algorithms in wireless networks involving games, the users need to know the channel gain of other users for finding their best response. Sometimes, the designer also need to know the channel gains of all the users to find the prices and allocations. We address all these limited information cases in this thesis to make our results realistic to the existing networks. In the later part of the thesis, we relax the information assumptions in the first part and use learning methods and Bayesian analysis.

1.4 Literature Review

1.4.1 Power Control Games

An Iterative Water Filling (IWF) algorithm is proposed in [120] to maximize the sum rate in the presence of individual power constraints in a Gaussian Multiple Access Channel (GMAC). This algorithm converges to a non-pareto-optimal Nash equilibrium and inefficient sum rate when the independent and strategic users take their power levels in a distributed fashion. Pricing of transmit power for Pareto improvement of the inefficient Nash equilibrium in noncooperative power control game is introduced in [100]. The pricing function is linear in transmit power and the utility of users are defined in terms of bits per Joule. In [78], the Nash equilibrium for a multi-carrier CDMA game is charac-

terized. There is no pricing to move the NE to the desired point and the utility function they consider are one to obtain the energy efficiency. A distributed pricing mechanism for interference coupled systems in which each user announces a price is proposed in [58]. The price signal from each user reflects the interference compensation price paid by the other users. In [114], a pricing based game for spectrum allocation with individual power constraint and multiple carriers is analyzed and a Price based Iterative Water Filling is proposed. The social optimization problem is taken as the weighted sum of Shannon capacities which are the utilities of individual users. To enable the users to achieve better Nash equilibrium a price based iterative distributed water-filling algorithm is proposed in [114]. In [38], a modified Vicrey-Clarke-Groves (VCG) mechanism is obtained for allocation of a divisible resource in which the pricing function is modified for achieving efficiency, individual rationality and almost budget balance properties.

Myerson [86] introduced optimal auctions in which the designer knowing the distribution of private values of players maximizes the expected revenue. In [40], for a wide-band wireless network that employs CDMA as the spectrum access mechanism, the revenue maximization problem is formulated as a Stackelberg game. The optimal prices are obtained for the Nash equilibrium points. For revenue maximization in a similar setting, suboptimal constant distributed pricing scheme is proposed in [93]. In [1], for a general delay network, a two-stage dynamic pricing-congestion game in which the service provider sets a price anticipating demand of users and users chose their flow vectors given the prices, is analyzed. An optimal revenue maximizing pricing is proposed for networks with several competing oligopolies and the extent of inefficiency loss is lower bounded. In [103], a lower bound for the ratio between the revenue from flat entre fee pricing rule and maximum revenue possible is provided, which they refer to as the Price of Simplicity (PoS). A price discrimination scheme is also studied and Price of Simplicity is obtained for it.

Recently, researchers have become more aware of environmental concerns and the need for **energy efficient** protocols [66]. In [78], a game theoretic model is proposed for energy efficient power control by defining utility of users as the ratio of throughput(goodput) and power (with unit bit/J) for multi-carrier CDMA wireless systems. A repeated game model and the cooperation induced due to repeated interaction is analyzed in [16].

In [116], a pricing game is considered within a multi-hop relay network where link cost functions depend only on the traffic flow rate. Each relay submits to the Source a charging function and a demand for a traffic share. The paper [117] investigates pricing games with both complete and incomplete information within multihop wireless networks, without taking into account the interference coupling between relays. For the complete information case, it is shown that all NE's are efficient and that there exists an efficient NE where each relay uses a charging function which depends linearly on the traffic flow rate. In [30], cooperative relaying is considered where the relays are incentivized to forward packets within a Stackelberg game framework. A bargaining game with utility requirements is considered for the same scenario in[28]. In another relevant work, the authors of [58] proposed, within a wireless ad hoc network setting, an asynchronous pricing algorithm in which each user cooperatively announces a price

to which all users respond by adjusting their transmission powers. The price announced by each user reflects its sensitivity to the interference created by other users.

1.4.2 Location Privacy

A wireless location privacy protecting system is analyzed and an information theoretic approach to define anonymity is proposed in [59]. In [61], the interaction between the local adversary deploying eavesdropping stations to track mobile users and mobile users deploying mix zones to protect their location privacy is studied using a game-theoretic model. MobiAd, a system for personalized, localized and targeted advertising on smart phones is proposed in [60]. Utilizing the rich set of information available on the phone, MobiAd presents the user with local advertisements in a privacy-preserving way by routing the information through a delay tolerant network. In this work they suggest the service provider to give discounts to motivate users to use MobiAd system.

1.4.3 Learning and Iterative methods in Game theory

In [67], an iterative algorithm is proposed for VCG and scalar parameterized VCG mechanisms which reduces the amount of overhead information by appropriate selection of the initial value of bids. The appropriate selection takes into account the previous bids and plays an important role in convergence to a NE. But they do not attempt any learning of the utility function. An iterative auction *iBundle* [90] is proposed in a setting in which users take myopic best-response bidding as response to the bid of other users and rules set by the designer. The optimality of proposed iterative auction is proved with connection to primal-dual optimization theory. In [14], the authors reduce mechanism design problems to standard algorithmic problems using techniques from sample complexity. The approach in [52] considers a learning phase followed by an accepting phase, and is careful to handle incentive issues for agents in both the phases. They study a limited-supply online auction problem, and construct value- and time-strategyproof auctions. The scenario when the users are strategic and they may manipulate the labeling for their individual benefit is considered in [42].

1.4.4 Malicious Behavior in Games and Mechanisms

In networked systems with selfish users, a loss in overall social welfare was identified and referred to as *Price of Anarchy* in [71, 96]. In [84],with the presence of malicious users this concept was extended and *Price of Byzantine Anarchy* and *Price of Malice* were first introduced and obtained bounds on these metrics, which are parametrized by the number of malicious users for a virus inoculation game in social networks. A modified definition was proposed in [12] 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 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 [12]. In [95], a more general definition of Price of Malice was 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 was introduced in [111], where the authors derived a bound on the damage caused by the malicious players. In [31], partial altruism of some of the users was analyzed and a bound on Price of Anarchy was obtained as a function of the altruism parameter. In [10], the Degree of Cooperation of a user as a vector of values was used to obtain a convex combination of other user utilities and to model altruistic behavior in the context of network routing games. The Value of Unilateral Altruism (VoU) was 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 was calculated for routing games in [11].

In order to circumvent *Price of Anarchy*, a pricing scheme for price taking users [70, 5, 18] and auctions for price anticipating users [75, 65] were developed. In [27], the effect of spiteful behavior of some of the users was analyzed in the context of first and second price auctions and the revenues obtained from each were compared. A Bayesian Nash equilibrium is obtained. A similar analysis was carried out in [110].

There are works in mechanism design literature, e.g. [56, 29, 7], 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 developed group-strategy proof mechanisms which are resistant to collusion and estimate the effect of collusion on overall efficiency and revenue. Price of Collusion was introduced in [54] 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 [6] and obtained in the context of load balancing games.

To counter the adversarial behavior, Micali & Valiant in [80], developed a modified Vickrey-Clarke-Groves (VCG) mechanism, taking into account collusive, irrational, and adversarial user 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. The First Price auction was modified to make it incentive compatible to adversarial behavior and other externality effects in [87].

There has been a lot of work on games and mechanisms with incomplete information. Games with Bayesian players have been studied a lot in works starting with [53]. Correlated equilibria in the context of incomplete information about other players, where the probabilities reflect the uncertainty about other players, were investigated in [8]. Recently there has been an increasing interest to analyze the security problems using game theory [76, 115]. Jamming problems are investigated using game theory in [118, 9].

1.4.5 Bayesian Mechanisms

In [73], an attack, by botnets composed entirely of mobile phones, using selected service request of user location in the network is studied. Through measurement, simulation and analysis, the authors in [73] have demonstrated the ability of a botnet composed of as few as 11,750 compromised mobile phones to degrade service to area-code-sized

regions by 93 percent. In [98], Bayesian jamming games are considered and the NE points for different jamming scenarios are obtained. Some of the works on anomaly based detection for mobile botnets are [15], [113] & [97]. While allocating resources to the users the base station or service provider should ensure QoS requirement of each user even in the presence of malicious users in the network [77].

1.5 Contributions of the Dissertation

The contributions of this thesis are,

1. A framework for designing mechanisms with and without malicious users in interference coupled networks. A new modelling of utility functions of malicious users in network resource allocation problems.

2. Mechanisms for multi-carrier systems, where the designer without knowing users utility functions achieves three different global objectives through appropriate pricing. Also pricing function for efficient joint power and rate allocation in multihop wireless networks.

3. A privacy mechanism where the company motivates users to report their location information at a granularity level desired by the company.

4. The convergence proof of the iterative distributed algorithm for implementation of the pricing mechanism.

5. Showing the effect of malicious behavior in VCG Mechanism for allocation of divisible resources and quantifying the Price of Malice and related metrics in VCG Mechanism and in various network mechanisms with adversarial users.

6. Analyzing the resistance of mechanisms against collusion of players, i.e. whether it is group strategy-proof or not. Defining and calculating metrics to quantify the effect of collusive behavior of malicious users in network mechanisms.

7. Design of differentiated pricing scheme to punish adversarial users. Also differentiated pricing using Bayesian information where the designer does not know the identities of the malicious users for determining the prices.

8. Bayesian analysis in which the users do not know the nature of other users. The users take action according to probability beliefs of others types (natures). The model is also extended to arbitrary number of malicious users in an ad-hoc wireless network. We find, in which scenarios, the uncertainty about the types is beneficial for the regular users.

9. A truthful Bayesian mechanism and quantification of the additional price paid by the malicious users, when they report false degree of maliciousness.

10. Detection methods based on hypothesis tests and machine learning algorithms for the detection of bots, observing the prices and rate allocations. These detections are used by the designer and regular users to construct a better estimate of the probability of existence of malicious users.

1.6 Outline of the Dissertation

First, in Chapter 2, we give the network mechanism model, interference function model and utility model with malicious users. We describe the different entities in the model, their interaction with the information available in the hands of each of them and assumptions about the different functions associated with these entities. A new modeling of malicious user utility function is proposed and a metric PoM for quantifying the effect of malicious users in the network is defined. Next in Chapter 3, as a first step, we design pricing mechanism for efficient power allocation in a multi-carrier Code Division Multiple Access(MC-CDMA) uplink. The users are assumed to be price taking. Pricing functions are obtained for different network level goals. The mechanism is extended to sum power constraint over the users and carriers. An iterative algorithm is proposed for the implementation of the pricing mechanism. We also consider multihop wireless networks with Femto cell relays and pricing mechanisms are designed for this case. The optimal incentives to the relays to carry the packets to the macro users under the femtocells from Macro Base Station (MBS) are proposed. The efficiency loss when the pricing is only a function of the amount of traffic, as in wired network, is quantified. In Chapter 4, we use the pricing mechanism framework which was proposed in the previous chapter, to design a location privacy mechanism for mobile commerce with entropy based user utility functions. The designer or company wants to improve the precision of location information from each user, which is captured by a designer objective function that maximizes the sum of granularity of information of all the users. For this the designer finds the optimal subsidies for the users with a budget constraint. Then in Chapter 5, a regression learning method is used by the designer to learn the utility functions of users from their actions, unlike in direct mechanisms where the designer asks the users to report their utility functions. Additionally, the convergence of the iterative distributed algorithm proposed in Chapter 3 is proven. Next in Chapter 6, the mechanism model with malicious users is described. A centralized auction mechanism with price anticipating users is proposed and its efficiency is proven. Then the values of PoM for auction mechanisms with malicious users are obtained with and without interference coupled utility functions. Another malicious behavior resulting from the collusion of many users to manipulate the mechanism is also analyzed. Next, both the pricing and auction mechanisms are extended for countering the malicious users. Next in Chapter 7, we relax the assumption that the users and the designer know the nature of users and we design Bayesian mechanisms. The conditions under which the uncertainty about the nature of the users is beneficial for the regular users and designer are obtained by comparing Bayesian case to the complete information case. Then pricing mechanisms with malicious users are extended to a case where each user submits a QoS requirement.

The dissertation ends with concluding remarks and discussion in Chapter 8.

Notation

Throughout the thesis, we denote vectors with boldface letters and scalars with italics. The vector of elements other than i^{th} element in vector $\mathbf{x}$ is denoted $\mathbf{x}_{-i}$. We let $f(x_i; \mathbf{x}_{-i})$ denote the function $f(.)$ as a function of x_i while keeping the vector components $\mathbf{x}_{-i}$ fixed. The logarithm denoted by log is to base 2. Analogously, $\exp(x)$ denotes 2^x.

Bibliographic Note

Portions of the content of Chapter 3 appeared in the papers [39], [33] and [69]. Portions of the content of Chapters 4, 5, 6 and 7 appear in the papers [34], [32], [37] and [36] respectively.

2 Preliminaries

In this chapter, we describe the system model and the assumptions about the strategy space of users, the utility functions of the users, the information available for different entities and the infrastructure of the network. We first give the system model with only selfish users and later extend it to include malicious users.

2.1 System Model

Consider a mechanism design model where a *designer* D influences a set, $\mathscr{A}$ of users who have private utilities (preferences) and compete for limited resources. The designer tries to achieve a global objective such as welfare maximization by making the users reveal their true utilities. For this purpose, the designer imposes certain rules and prices to the users who agree to participate in the mechanism. However, the designer cannot dictate user actions or modify their private utilities. This setup is applicable to a variety of network resource allocation problems in networks such as flow and power control, interference management, and spectrum sharing.

In order to analyze such mechanisms, define an N-player *strategic game* which results due to the interaction of users, $\mathscr{G}(\mathscr{A}, x \in \mathscr{X}, U)$, where each user or player $i \in \mathscr{A}$ has a respective scalar **decision variable** x_i such that

$$\mathbf{x} = [x_1, \ldots, x_N] \in \mathscr{X} \subset \Re_+^N,$$

and $\mathscr{X}$ is the decision space of all players. The decision variable x_i may represent, depending on the specific problem formulation, i^{th} player's flow rate, power level, investment, or bidding in an auction.

Assumption 2.1. *We assumes that the strategy space $\mathscr{X}$ has scalar decision variables, is compact, convex and has a nonempty interior.*

Due to the inherent coupling between the players, the decisions of players directly affect each others performance as well as the aggregate allocation of limited resources. For example, the players may share fixed divisible resource X_{max}, such that $\sum_i x_i \leq X_{max}$. In the context of power control, x_i denotes the received power of user i. The transmitted power of user i is $\frac{x_i}{h_i}$ where h_i is the channel gain.

The **preference** of the i^{th} player is captured by the utility function

$$U_i(\mathbf{x}) : \mathscr{X} \to \Re.$$

Assumption 2.2. *The utility function of the i^{th} user, $U_i(\boldsymbol{x})$, is jointly continuous in all its arguments and twice continuously differentiable, non-decreasing and strictly concave in x_i.*

The designer imposes a price $C_i(\mathbf{x})$ on the actions of players, which is formulated by adding it as a cost term to utility.

Assumption 2.3. *The payment function of the i^{th} user, $C_i(\boldsymbol{x})$, is jointly continuous in all its arguments and twice continuously differentiable, non-decreasing and convex in x_i.*

The player i has the cost function

$$J_i(\mathbf{x}) = C_i(\mathbf{x}) - U_i(\mathbf{x}), \tag{2.1}$$

and solves the individual optimization problem

$$\min_{x_i} J_i(\mathbf{x}). \tag{2.2}$$

Assumption 2.4. *The cost function of the i^{th} user, $J_i(\mathbf{x})$, is twice continuously differentiable in all its arguments and strictly convex in x_i.*

The **Nash equilibrium** (NE) is a widely-accepted and useful solution concept in strategic games, where no player has an incentive to deviate from it while others play according to their NE strategies.

Definition 2.5 (Nash Equilibrium)**.** The strategy profile $\mathbf{x}^* = [x_1^*, \ldots, x_N^*]$ is in Nash Equilibrium if the cost of each player is minimized at the equilibrium given the best strategies of other players.

$$J_i(x_i^*, \mathbf{x}_{-i}^*) \leq J_i(x_i, \mathbf{x}_{-i}^*), \forall i \in \mathscr{A}, x_i \in \mathscr{X}_i$$

The NE is at the same time the intersection point of player's best responses obtained by solving (2.2) individually, i.e.,

$$x_i^* := \arg\min_{x_i} J_i(x_i, \mathbf{x}_{-i}^*), \forall i, \tag{2.3}$$

Definition 2.6 (Dominant Strategy Equilibrium)**.** The strategy profile $\mathbf{x}^D = [x_1^D, \ldots, x_N^D]$ is in dominant strategy equilibrium if the cost of each player is minimized at the equilibrium irrespective of the strategies of other players.

$$J_i(x_i^D, \mathbf{x}_{-i}) \leq J_i(x_i, \mathbf{x}_{-i}), \forall i \in \mathscr{A}, x_i \in \mathscr{X}_i, \mathbf{x}_{-i} \in \mathscr{X}_{-i}$$

The players choose the dominant strategy regardless of the actions of others. Hence, DSE is a stronger concept and a subset of NE and doesn't require information about the utility or action of other users.

We consider two types of users in this thesis.

Definition 2.7 (Price anticipating users)**.** Price anticipating users consider the effect of their strategy on the allocation and pricing functions while deciding on their strategy.

Definition 2.8 (Price taking users)**.** Price taking users consider allocation and pricing functions as constants while taking their best response.

Price taking users ignore the effect of their strategy mainly due to lack of information and less computational capacity. When the users are price taking the equilibrium obtained according to equation (2.3) is referred as competitive equilibrium [65].

2.1.1 Mechanism Design

Definition 2.9 (Mechanism)**.** A mechanism $\mathscr{M}$ is a tuple $(\mathscr{X}_1, \mathscr{X}_2, \cdots, \mathscr{X}_N, f(.))$, where function f specify an outcome for every strategy vector $\mathbf{x} \in \mathscr{X} \subset \Re^N$, of the players.

The function f is implemented through allocation and pricing rules.

We differentiate between two kinds of mechanisms, auctions and pricing, which differ in the assumption on the nature of the users and the interaction rules.

Definition 2.10 (Auction Mechanism)**.** In auction mechanisms, the designer D imposes on a price anticipating user $i \in \mathscr{A}$ a (possibly user-specific)

- resource allocation rule, $Q_i(\mathbf{x})$,
- resource pricing, $C_i(\mathbf{x})$,

based on user bids $\mathbf{x}$. In auctions, $f(\mathbf{x}) = (Q_1(\mathbf{x}), Q_2(\mathbf{x}), \cdots, Q_N(\mathbf{x}), C_1(\mathbf{x}), C_2(\mathbf{x}), \cdots, C_N(\mathbf{x}))$.

The users who are price anticipating decide on their bid by minimizing their individual costs.

Definition 2.11 (Pricing Mechanism)**.** In pricing mechanisms, the price taking users decide on their allocation as a best response to the (user-specific) price P_i induced by the designer and there is no explicit allocation rule dictated.

In the pricing mechanism case, the cost function is

$$J_i(\mathbf{x}) = P_i x_i - U_i(\mathbf{x}) \, \forall i. \tag{2.4}$$

The **designer objective**, e.g. maximization of aggregate user utilities or social welfare, can be formulated using an objective function

$$V(\mathbf{x}, U_i(\mathbf{x}), C_i(\mathbf{x})) : \mathscr{X} \to \Re,$$

where $C_i(\mathbf{x})$ and $U_i(\mathbf{x})$, $i = 1, \ldots, N$ are user-specific pricing terms and player utilities, respectively. Thus, the objective function V characterizes the desirability of an outcome $\mathbf{x}$ from the designers perspective. In some cases when the designer objective is to satisfy certain minimum performance constraints such as players achieving certain quality-of-service levels, the objective can be characterized by a region (a subset of the game domain $\mathscr{X}$). For the net utility maximization, the designer objective is

$$V(\mathbf{x}) = \sum_{i \in \mathscr{A}} U_i(\mathbf{x}), \tag{2.5}$$

The properties of a mechanism and their corresponding game counterparts are summarized in Table 2.1.1 and in the following definitions. Now we formally define the properties of the mechanisms.

Table 2.1: Mechanism Design Objectives

Mechanism Property	*Corresponding Game Property*
Efficiency	NE coincides with maximum of objective function
Strategy-Proofness	Game admits a truth revealing dominant strategy equilibrium
Budget balance	No net payments at the NE
Individual Rationality	Utility of all agents should be greater than or equal to zero

Definition 2.12 (Efficiency)**.** Efficient mechanisms maximize designer objective at the equilibrium point of the corresponding game, i.e. they solve the problem,

$$\mathbf{x}^* = \arg\max_{\mathbf{x}\in\mathscr{X}} V(\mathbf{x}, U_i(\mathbf{x}), C_i(\mathbf{x})).$$

Definition 2.13 (Strategy-proof)**.** A mechanism is said to be strategy-proof, if and only if, the corresponding game admits a DSE that reveals the true user types (preferences).

$$C_i(\mathbf{x}^D) - U_i(\mathbf{x}^D) \leq C_i(\mathbf{x}^D) - \tilde{U}_i(\mathbf{x}^D),\ \forall \tilde{U}_i, \forall i. \tag{2.6}$$

where U is the true utility and $\tilde{U}$ is the misrepresented utility.

Definition 2.14 (Individual Rationality (or) Voluntary Participation (VP))**.** This property ensures that the utility of all agents at the NE should be greater than or equal to the utility they would get by dropping out of the mechanism. The utility that agents get by not participating in the mechanism is usually taken to be zero, i.e.

$$J_i(\mathbf{x}^*) \leq 0,\ \forall i \in \mathscr{A}. \tag{2.7}$$

Definition 2.15 (Budget Balance)**.** A mechanism is called budget balanced if the net payments at the NE add up to zero regardless of user preferences, i.e. $\sum_{i\in\mathscr{A}} C_i(\mathbf{x}^*) = 0$.

The mechanisms need not satisfy some of these properties. A metric which is widely used in the literature to measure the efficiency loss in a mechanism is PoA.

Definition 2.16 (Price of Anarchy(PoA))**.** The metric Price of Anarchy(PoA) [71] of a mechanism $\mathscr{M}$ is defined as:

$$PoA(\mathscr{M}) := \frac{\sum_{j\in\mathscr{A}} U_j(\mathbf{x}^*}{\sum_{j\in\mathscr{A}} U_j(\mathbf{x}')},$$

where $\mathbf{x}'$ is the efficient point and $\mathbf{x}^*$ is the Nash equilibrium.

2.1.2 Interference Function Model

Signal-to-Interference and Noise Ratio (SINR) of the received signal is

$$\gamma_i(\mathbf{x}) = \frac{x_i}{I_i(\mathbf{x})}, \tag{2.8}$$

where $I_i(x)$ denote the interference function. In the next chapters we consider SINR based utility functions for users.

Yates in [119] proposed *standard* interference functions using an axiomatic approach. A different class of functions known as *general* interference functions were proposed in [24] and defined as follows.

Definition 2.17 (General interference functions)**.** These are interference functions, $I : \Re_+^{K+1} \rightarrow \Re_+$, which satisfy following properties,
A1 conditional positivity: $I(\mathbf{x}) > 0$ if $\mathbf{x} > 0$
A2 scale invariance: $I(\alpha\mathbf{x}) = \alpha I(\mathbf{x}), \forall \alpha \in \Re_+$
A3 monotonicity: $I(\mathbf{x}) \geq I(\tilde{\mathbf{x}})$ if $\mathbf{x} \geq \tilde{\mathbf{x}}$
A4 strict monotonicity: $I(\mathbf{x}) > I(\tilde{\mathbf{x}})$ if $\mathbf{x} \geq \tilde{\mathbf{x}}, x_{N+1} \geq \tilde{x}_{N+1}$.

In [25], both the framework in [119] and the framework of general interference functions were compared and it was proved that every standard interference function is a special case of general interference functions. This means that any problem involving standard interference functions can be reformulated in terms of the general framework axioms $A1, A2 \text{and} A3$. Therefore, the structural results obtained for general interference functions in [23] and [22] can be applied also for standard interference functions.

The class of *log-convex* interference functions [22] are a subset of general interference functions. They satisfy $A1 - A3$ and additionally $I(e^x)$ is log-convex on $\Re^{N+1}$. In [23], it was proven that every convex interference function is a log-convex interference function, however the converse is not true.

Most resource allocation problems such as weighted utility maximisation are found to be not jointly concave or convex in the power domain. So the aim is to characterize a strictly monotonic increasing and twice continuously differentiable transformation $\psi(s) = x$ which can convexify these resource allocation problems.

The linear interference functions which is a sub-class of log-convex interference function is given by,

$$I_i(\mathbf{x}) = \sum_{j \neq i} x_j + \sigma^2,$$

where σ represents the background noise. In the case of linear interference functions the transformation $x_i = \exp(s_i)$ is the unique transformation which transforms the weighted utility maximisation and other commonly occurring optimization problems to be jointly convex or concave [20]. Now we check whether this exponential transformation works or not when we relax the condition of linear interference functions to other kinds of interference coupling.

The largest class of interference functions, which preserves concavity of resource allocation strategies of interference coupled wireless systems is the family of log-convex interference functions [20].

Now we define certain class of utility functions of users.

Definition 2.18. *Conc* is the family of monotonically increasing, differentiable and concave utility functions. *EConc* is the family of monotonically increasing and differentiable functions U for which $U(\exp\{x\})$ is concave.

Based on the results obtained for linear interference functions and utility functions in the family *Conc*, we consider a subset *EConc* of *Conc*. It was shown that the family of exponential transformation is the unique transformation, such that relevant and frequently encountered problems in interference coupled wireless systems are jointly concave on the s- domain [20]. This is true for linear interference functions and for all utility functions in the class *EConc*. In this thesis, we focus on linear interference functions based utility functions in the class *EConc*.

2.1.3 Mechanism Design Model with Heterogeneous Users

We consider mechanisms with malicious users from Chapter 6 onwards. In this section, we introduce the utility function model of the heterogeneous users. The utility functions of malicious users can be very different depending on their nature and goals. One subset of users have 'abnormal' utility functions compared to the remaining set of 'regular' selfish users. The disrupting nature of malicious users, who want to cause a loss to other users even at the cost of their own benefit, and the altruistic nature of some users, who want to care for the social welfare at their own cost, are captured using *modified* utility functions. One such modified utility function is obtained by a convex combination of user utilities

$$U_i^m(\mathbf{x}, \theta_i) = U_i(\mathbf{x}) + \theta_i \sum_{j \neq i} U_j(\mathbf{x}), \tag{2.9}$$

where the parameter θ_i is between -1 and 1, and captures the range of behavior of user i. This utility function can be modified by taking the average of the utilities of all the users in the second term ([31]). Unlike in [10], 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
$\theta > 0$	altruistic
$\theta = 0$	selfish
$\theta < 0$	malicious

Let us define the set of selfish users as $\mathscr{S} \subset \mathscr{A}$. In addition, the set of both malicious and altruistic users, i.e. users with $\theta_i \neq 0$ is defined as $\mathscr{B} := \mathscr{A} \backslash \mathscr{S}$. When the set $\mathscr{B}$

has only malicious users, the utility function of malicious users can be modified as

$$U_i^m(\mathbf{x}, \theta_i) = U_i(\mathbf{x}) + \theta_i \sum_{j \in \mathscr{S}} U_j(\mathbf{x}),\ \forall i \in \mathscr{B}. \tag{2.10}$$

A formal definition of malicious user is given next.

Definition 2.19. A malicious user is a user who has a utility function given in (2.10) with degree of maliciousness $-1 \leq \theta < 0$.

A jammer transmits with higher power in the same band as regular users to create interference to other users. The impact of the interference a jammer creates, on other users, is modeled by the second term of Equation 2. Note that the interference power comes in the denominator of the second term and the jammer tries to increase that while maximizing the utility in the Equation 2. The equation can not model all the jamming scenarios especially when the jammer does not want to have useful transmission for himself or any other users as in [101].

In the physical layer secrecy problem, the malicious user jams the wireless network such that both the regular and malicious transmission cannot be decoded at the receiver[101]. The malicious users identities can not be detected by the network because the whole network is jammed. The kind of extreme behavior, where the malicious users are not selfish and rational, cannot be modeled by the SINR model in equation (2.9). This is because the malicious users do not want to have useful transmission for themselves or any other users. Even if there is positive SINR at the base station receivers, the secrecy capacity is zero and no one is able to have successful reception[102]. In our model, we assume that the malicious users want to transmit something useful in the same way as the regular users with positive capacity. This kind of *weak* malicious behavior enables the malicious users to act like regular users without being detected.

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 some utility functions and values of θ. For concavity the utility functions should satisfy following condition:

$$\frac{d^2U_i}{dx_i^2} + \theta_i \sum_{j \neq i} \frac{d^2U_j}{dx_i^2} \leq 0,\ \text{for} - 1 \leq \theta_i \leq 1, \forall i. \tag{2.11}$$

We start our analysis with general concave utility functions for the users. However, in order to ensure the existence of at least one NE, we use the utility functions which satisfy the condition in equation (2.11).

Assumption 2.20. *The modified utility function of the i^{th} user, $U_i^m(\mathbf{x})$ is jointly continuous in all its arguments and twice continuously differentiable, nondecreasing and strictly concave (utility function $U_i(\mathbf{x})$ satisfies the condition in equation (2.11)) in x_i.*

The utility function of malicious user without self utility is

$$U_i^m(\mathbf{x}, \theta_i) = \theta_i \sum_{j \in \mathscr{S}} U_j(\mathbf{x}),\ \forall i \in \mathscr{B}, \tag{2.12}$$

An alternate utility function,

$$U_i^m(\mathbf{x}, \theta_i) = (1 - |\theta_i|)U_i(\mathbf{x}) + \theta_i \sum_{j \in \mathscr{S}} U_j(\mathbf{x}),\ \forall i \in \mathscr{B}, \tag{2.13}$$

models the user behavior with a gradual decrease in the self utility when $|\theta|$ increases. In the case of network resource allocation, the malicious users take disproportionate higher share of resources and thereby reduce the utility of other users. This model does not capture such a malicious behavior because it will not yield to a disproportionate higher share of resource to malicious user. This observation is demonstrated for a specific example later in Section 6.2.3. In the case of network resource allocation, equation (2.13) is not appropriate for modeling malicious behavior and therefore the malicious modeling in equation (2.10) is adopted in this thesis. Nevertheless, the model in equation (2.13) is still a useful one for modeling extreme altruistic behavior.

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

Price of Malice ($PoM(\mathscr{M})$) is another form of PoA metric, defined in Definition 2.16, which does not focus on the overall efficiency but the efficiency loss of the set of selfish users. We redefine the metric $PoM(\mathscr{M})$ of mechanism $\mathscr{M}$ in order to make it suitable for resource sharing mechanisms. In [12], for congestion games with malicious flow concentrated on one malicious player, Price of Malice was defined, based on the delay experienced at Nash equilibrium point with and without the malicious player. We now redefine PoM for network games and mechanisms with discrete set of players similar to the definition given in [12].

Definition 2.21 (Price of Malice(PoM))**.** The metric Price of Malice(PoM) of a mechanism $\mathscr{M}$ is defined as:

$$PoM(\mathscr{M}) := \frac{\sum_{j \in S} U_j(\tilde{\mathbf{x}}) - \sum_{j \in S} U_j(\mathbf{x}^*)}{\sum_{j \in S} U_j(\tilde{\mathbf{x}})},$$

where $\tilde{\mathbf{x}}$ is the Nash equilibrium when none of the users are malicious and $\mathbf{x}^*$ is Nash equilibrium in the presence of malicious users.

2.2 Information and Infrastructure Assumptions

The users share and compete for limited resources in the given environment under its information, infrastructure and communication constraints. Now we list the assumptions we take in different chapters of this dissertation about the information available to different agents of the mechanism and the infrastructure available in the network. Throughout the dissertation, we assume that there is a central authority (designer) which can be the base station or operator, who exerts some level of control over the users. The users and the designer are assumed to have complete channel state information in the chapters 3,

5 and 6. We consider adhoc wireless networks with CDMA or OFDM scheme and single hop in most part of the dissertation. In Section 3.6, we consider multihop wireless network where the network has Femto cell relays which forward the data from the Macro base station to the macro users. We assume that designer does not know the utility functions of users but compute the prices and allocations using the one dimensional signals from them. In Chapter 5, we consider a case where the designer learns the utility functions of users from their signals.

In chapters 3, 4 and 5, the network has only regular selfish users who are interested only in their own utilities. In chapters 6 and 7, we consider network with heterogeneous users. Till the Chapter 6, the users and the designer know exactly the nature of the users and the identities of the malicious user. In the chapter 7, we relax this assumption and analyze the case where the users and the designer have Bayesian information about the nature.

Chapter	**Kind of Mechanism**
3, 4, 6 and 7	Distributed, indirect mechanism with price taking users
6 and 7	Centralized, indirect mechanism with price anticipating users
7(Section 7.6)	Centralized, direct mechanism with price anticipating users

Table 2.2: Different Kinds of Mechanisms in the Dissertation

Table 2.2 gives the different kinds of mechanisms we consider in the different chapters of the dissertation. In direct mechanisms, the users report their type directly and get power allocation and pricing in return. In indirect mechanisms, the users bid a value and power allocation and pricing are computed by the designer based on their bids.

3 Pricing Mechanisms for Resource Allocation in Wireless Networks

In this chapter, we consider resource allocation in interference coupled wireless networks with strategic price taking users.

3.1 Introduction

The users decide independently on their power levels without revealing their utility functions, so as to maximize their individual utilities. Concurrently, the base station has a social goal such as weighted social welfare (weighted sum of user utility) maximization or energy minimization, which may not be achieved due to this strategic behavior of users. This is because at the Nash Equilibrium (NE) point of the underlying noncooperative power control game, there is a misalignment of social and individual user objectives. This phenomena is known as Price of Anarchy is defined in the previous chapter. To counter this scenario, the base station acts as a mechanism designer and uses **pricing schemes** [55] to incentivize the users.

A single cell multi-carrier CDMA system is depicted in the Figure 3.1. The symbol of different users are spread over multiple subcarriers which are phase shifted according to orthogonal code values. We study distributed pricing schemes in which the users decide on their power levels over each channel depending on their utility functions and the designer sets the prices over different channels.

We consider a general convex constraint set but concentrate on individual power constraints for each user, which make the power allocation non-trivial even for single carrier systems due to the interference coupling between the users. In comparison, the separable user utility function in wireline case results in full allocation for all. Additional constraint on the total power over each channel and total power constraint on all the channels and users, are considered for multi-carrier systems. The designer iteratively adjusts the dual variables Lagrange multipliers corresponding to different power constraints, which are used to modify the prices, to bring the system to an efficient point. In this work we extend Kelly pricing mechanism [70] which are for network with uncoupled utilities, for interference coupled systems. Author in [64] proves that in a network with price taking users with uncoupled utilities, there exists a market clearing price which ensures efficient resource allocation. In this chapter, we propose optimal prices for wireless network with price taking users with interference coupled utilities.

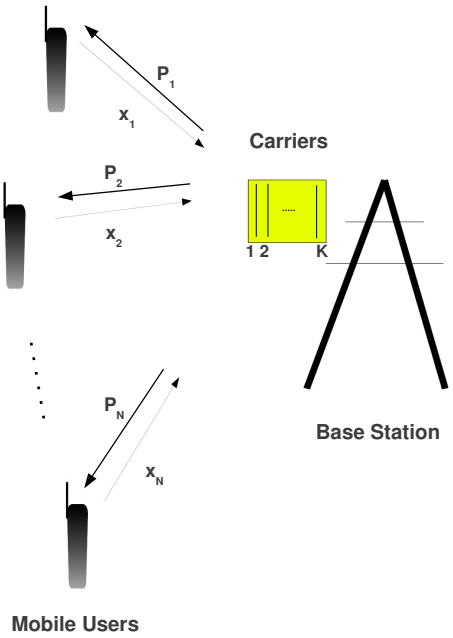

Figure 3.1: A multiuser multi-carrier single cell wireless system where users choose power level over different carriers and the base station assigns prices to the users.

We propose mechanisms for multi-carrier systems, where the designer without knowing users utility functions achieve different designer objectives through appropriate pricing. The pricing mechanisms obtained here can be implemented through a distributed iterative algorithm rather than existing heuristic suboptimal or centralized algorithms.

In this chapter, we propose mechanisms for multi-carrier systems, where the designer – without knowing users utility functions– achieves two different global objectives through appropriate pricing. The pricing mechanisms obtained here can be implemented through a distributed iterative algorithm rather than existing heuristic suboptimal or centralized algorithms. Unlike Kelly mechanism [70], the prices obtained in this chapter are not just the Lagrange multipliers but are solution of a linear program which has system parameters and Lagrange multipliers as coefficients.

We investigate mechanisms in which the user utility functions satisfy the Assumption 2.2. The users do not report their utility functions and just decide on their own power level. The users are not considered to be price anticipating here because in a distributed network there is an information asymmetry between the users and the designer. The users do not know the action and utility function of other users or the nature of pricing

function. Thus, they just adopt a best response strategy by *taking* the price given by the designer as a constant.

The work in this chapter is an extension of the work in [5] for multi-carrier systems with general concave user utility functions which is unknown to the designer and with individual user power constraints, individual channel constraint and a global power constraint.

In addition to pricing user transmit powers for obtaining social welfare, the designer may like to maximize the revenue obtained from these prices. We also design pricing mechanisms for designer **revenue maximization** which may lead to non optimal social welfare.

We consider in this chapter the scenario that the users care only for getting maximum throughput, but an external mechanism designer imposes prices to the users such that their energy consumption is decreased to improve overall energy efficiency of the system. Thus, the designer encourages users to be more energy conscious. We model energy efficiency objective by subtracting a *general convex function of the power levels* of users from the social welfare (sum of utilities of all users). This additional term is multiplied by a tuning parameter which allows smoothly varying the emphasis from the social welfare to the system energy efficiency.

We also consider multihop wireless network, where Femto Base Stations (FBSs) act as relay nodes, and are incentivized to carry traffic from a Macro Base Station (MBS) to Macro Users (MUs). Due to their ability to bring about massive spatial reuse of frequency, small cell base stations such as Femto Base Stations (FBS) or Pico Base Stations (PBS) are increasingly important for improving network capacity. At the same time, FBSs also give better data rate to end users due to short transmission range and fewer users per cell. FBSs are normally deployed in indoor home or office environments owned or rented by second parties other than the service provider, and are normally underutilized. One way to better utilize the capacities of FBSs is to employ the FBSs as relays. In this scenario, FBSs carry traffic from the Macro Base Station (MBS) to Macro Users (MUs), in addition to serving Femto Users (FUs). The relaying generates revenue for the owner of the FBSs. Moreover, the relaying extends the coverage of FBSs to outdoor environments [51], thereby reducing the burden on the MBS. We first examine the the global problem of jointly optimal allocation of traffic flow and transmission power in the multihop wireless network. We then examine a game in which selfish and strategic relays submit charging functions to the source and choose transmission powers over a MAC channel from the relays to the user. Relay charging functions are considered which yield efficient allocation at the Nash Equilibrium (NE) of the game.

In this chapter, we first consider different designer objectives and design appropriate mechanisms. Then we consider multihop small cell relay network and solve the power and rate allocation problem using pricing.

3.2 Pricing Mechanisms for Net Utility Maximization

We consider pricing mechanisms for net utility maximization in this section. We assume that in the global objective, different users are given weights according to their priorities.

3.2.1 Pricing Mechanism for Multi-carrier Systems

Let the superscript (n) is associated with the n^{th} carrier. Let each user i receive power $x_i^{(n)}$ and has price for transmission $P_i^{(n)}$, over a total of K carriers. Therefore, the total transmitted power of user i is $\sum_n \frac{x_i^{(n)}}{h_i^{(n)}}$ where $h_i^{(n)}$ is the channel gain user i experience over carrier n. For MC- CDMA system, with random spreading sequences, the output SINR of the the user with a Matched Filter (MF) receiver is given by [78],

$$\gamma_i^{(n)}(\mathbf{x}) = \frac{x_i^{(n)}}{\frac{1}{L}\sum_{j\neq i} x_j^{(n)} + \sigma^2}, \tag{3.1}$$

where L is the processing gain.

The net utility maximization objective of the designer is given in equation (2.5) of previous chapter. In multi-carrier systems with individual user, channel and total power constraint, the weighted net utility maximization objective of the designer is to solve the optimization,

$$\max_{\mathbf{x}} \sum_i w_i \sum_n (U_i(\gamma_i^{(n)}(\mathbf{x})),$$

subject to

$$\sum_n \frac{x_i^{(n)}}{h_i^{(n)}} \leq X_{max},\ \forall i, \sum_i \frac{x_i^{(n)}}{h_i^{(n)}} \leq X_c,\ \forall n, \tag{3.2}$$

and total power constraint given by

$$\sum_i \sum_n \frac{x_i^{(n)}}{h_i^{(n)}} \leq X_{total},$$

where X_{max} is the power constraint over each channel, X_c is the power constraint over each channel, X_{total} is the total power limit and w_i is the weight of user i. So the Lagrangian function of designer can be written as:

$$L = V(\mathbf{x}) - \sum_i \lambda_i (\sum_n \frac{x_i^{(n)}}{h_i^{(n)}} - X_{max}) - \sum_n \nu_n (\sum_i \frac{x_i^{(n)}}{h_i^{(n)}} - X_c) - \pi (\sum_i \sum_n \frac{x_i^{(n)}}{h_i^{(n)}} - X_{total}), \tag{3.3}$$

where λ_i's, ν_n's and π are nonnegative Lagrangian multipliers. The Karush-Kuhn-Tucker (K.K.T) conditions are given by:

$$w_i \frac{dU_i(\gamma_i^{(n)}(\mathbf{x}))}{dx_i^{(n)}} + \sum_{j\neq i} w_j \frac{dU_j(\gamma_j^{(n)}(\mathbf{x}))}{dx_i^{(n)}} - \frac{\lambda_i + \nu_n + \pi}{h_i^{(n)}} = 0,\ \forall\ i, n, \tag{3.4}$$

$$\lambda_i(\sum_n \frac{x_i^{(n)}}{h_i^{(n)}} - X_{max}) = 0, \forall i, \ \sum_n \frac{x_i^{(n)}}{h_i^{(n)}} \leq X_{max} \forall i.$$

$$\nu_n(\sum_i \frac{x_i^{(n)}}{h_i^{(n)}} - X_c) = 0, \forall i, \ \sum_i \frac{x_i^{(n)}}{h_i^{(n)}} \leq X_c \forall n.$$

$$\pi(\sum_i \sum_n \frac{x_i^{(n)}}{h_i^{(n)}} - X_{total}) = 0, \ \sum_i \sum_n \frac{x_i^{(n)}}{h_i^{(n)}} \leq X_{total} \forall n.$$

To solve the designer problem at the NE of the game prices are designed by the designer. Let $P_i^{(n)}$ be the price per received power of the user i on the n^{th} carrier. For multi-carrier systems the user optimization problem from equation (2.1) will be,

$$\max_{x_i} \ \sum_n (U_i(\gamma_i^{(n)}(\mathbf{x})) - x_i^{(n)} P_i^{(n)}).$$

The user best response obtained from first order derivative is

$$\frac{dU_i(\gamma_i^{(n)}(\mathbf{x}))}{dx_i^{(n)}} - P_i^{(n)} = 0, \text{ and } x_i^{(n)} = (\frac{dU_i^{(n)}}{dx_i^{(n)}})^{-1}(P_i^{(n)}), \forall \ i \in A, \forall \ n. \tag{3.5}$$

The equation (3.5) can be also written in terms of individual SINR as,

$$\frac{dU_i^{(n)}}{d\gamma_i^{(n)}} = \frac{P_i^{(n)}}{d\gamma_i^{(n)}/dx_i^{(n)}}, \ \forall \ i \in \mathscr{A}. \tag{3.6}$$

Using equation (2.8),

$$\frac{dU_i}{d\gamma_i^{(n)}} = P_i^{(n)} I_i^{(n)}, \ \forall \ i \in \mathscr{A}, \forall \ n. \tag{3.7}$$

The equation (3.4) can be rewritten as,

$$w_i \frac{dU_i}{dx_i^{(n)}} + \sum_{j \neq i} w_j \frac{dU_j}{d\gamma_j^{(n)}} \frac{d\gamma_j^{(n)}}{dx_i^{(n)}} - \frac{\lambda_i + \nu_n + \pi}{h_i^{(n)}} = 0, \ \forall i, n. \tag{3.8}$$

Aligning both the user problems and the global objective of the base station by substituting from the user equations in (3.5), the above equation becomes

$$w_i P_i^{(n)} - \sum_{j \neq i} w_j \frac{dU_j^{(n)}}{d\gamma_j^{(n)}} \frac{x_j^{(n)}}{(I_j^{(n)})^2} - \frac{\lambda_i + \nu_n + \pi}{h_i^{(n)}} = 0, \ \forall i, n. \tag{3.9}$$

By knowing the structure of user cost function and using (3.7), the designer can obtain the prices by solving

$$w_i P_i^{(n)} - \sum_{j \neq i} w_j \frac{P_j^{(n)} x_j^{(n)}}{I_j^{(n)}} - \frac{\lambda_i + \nu_n + \pi}{h_i^{(n)}} = 0, \ \forall i \in \mathscr{A}, n \tag{3.10}$$

The above system of equations can be written in matrix form as,

$$A^{(n)} \cdot P^{(n)} = B^{(n)} \cdot L, \ \forall n, \tag{3.11}$$

where $A^{(n)}$ and $B^{(n)}$ are defined accordingly.

$$A^{(n)} := \begin{pmatrix} w_1 & -w_2\gamma_2^{(n)} & \cdots & -w_N\gamma_N^{(n)} \\ -w_1\gamma_1^{(n)} & w_2 & \cdots & -w_N\gamma_N^{(n)} \\ \vdots & & \ddots & \vdots \\ -w_1\gamma_1^{(n)} & -w_2\gamma_2^{(n)} & \cdots & w_N \end{pmatrix}, \tag{3.12}$$

$$B^{(n)} := \begin{pmatrix} \frac{1}{h_1^{(n)}} & 0 & \cdots & 0 & \frac{1}{h_1^{(n)}} & \frac{1}{h_1^{(n)}} \\ 0 & \frac{1}{h_2^{(n)}} & \cdots & 0 & \frac{1}{h_2^{(n)}} & \frac{1}{h_2^{(n)}} \\ \vdots & & \ddots & \vdots & & \\ 0 & 0 & \cdots & \frac{1}{h_N^{(n)}} & \frac{1}{h_N^{(n)}} & \frac{1}{h_N^{(n)}} \end{pmatrix}, \tag{3.13}$$

and $L = [\lambda_1, \ldots, \lambda_N, \nu_n, \pi]^T$.

Remark 3.1. The implementation of this mechanism requires minimum information overhead. The designer only needs to observe the received power level vector $\mathbf{x}$ and the individual SIRs, γ, of players both of which are already available. The player i, in return only needs to know the price P_i . Finally, the computation of actual uplink power levels $\mathbf{p}$ can be carried from $\mathbf{x}$ using the measured channel gains.

3.2.2 Iterative Distributed Algorithm for Multi-Carrier Systems

We propose a gradient update iterative distributed algorithm to implement the pricing mechanism obtained above. A best response update of power levels by each user will require lot of system level information which may not be available to individual users. In the algorithm, the users are assumed to have *bounded rationality* property in which the decision for updates are taken based on previous decision, gradually and heuristically in a distributed fashion. In this case, the users just need to know the prices set by the designer according to (3.11) and $p_i(k+1) = T(p_i(k))$ where $T(.)$ is the transformation and k is the time step. We now define pricing mechanism $\mathscr{M}_b$, for which the prices and bids from user for each carrier can be obtained using iterative methods as following.

$$P^{(n)}(k+1) = (A^{(n)})^{-1}B^{(n)} \cdot L(k), \forall n \tag{3.14}$$

$$p_i^{(n)}(k+1) = [p_i^{(n)}(k) - \frac{\kappa_i}{h_i^{(n)}} \frac{\partial J_i}{\partial x_i^{(n)}}]^+ \ \ \forall i \in \mathscr{A}, \tag{3.15}$$

$$\lambda_i(k+1) = [\lambda_i(k) + \kappa_D\big(\sum_n p_i^{(n)}(k) - X_{max}\big)]_+, \ \ \forall i \in \mathscr{A} \tag{3.16}$$

$$\nu_n(k+1) = [\nu_n(k) + \kappa_D\big(\sum_i p_i^{(n)}(k) - X_c\big)]_+, \quad \forall n. \tag{3.17}$$

and

$$\pi(k+1) = [\pi(k) + \kappa_D\big(\sum_i \sum_n p_i^{(n)}(k+1) - X_{total}\big)]_+ \tag{3.18}$$

Since the designer optimization problem can be convexified and thus admits a unique solution, we can find unique λ's which align it to the user convex optimization problems. Hence, there exist corresponding prices, obtained from the matrix transformation given in (3.11), which will determine the optimal power levels. The algorithm which also shows the information flow for the iterative method is given below in Algorithm 1. It can be observed that the designer updates the prices after some time slots of power update. The convergence analysis of this algorithm is given in Chapter 5.

Algorithm 1: Iterative Pricing Mechanism $\mathscr{M}_b$

Input: *Designer (base station)*: Maximum power levels X_{max} and the designer objective
Input: *Players (users)*: Utilities U_i
Result: Optimum power levels p^* and SIRs γ^*

```
Initial power levels p(0) and prices P_i(0) ;
repeat
    begin Designer:
        Observe player power levels p ;
        Compute the matrices A^(n) and B^(n) Update λ's according to (3.16) ;
        foreach Channel n do
            Update prices P^(n) according to (3.14).
        end
        Send each user i respective channel prices P_i^(n). begin Players:
            foreach Player i do
                foreach Channel n do
                    Estimate marginal utility ∂U_i(x)/∂x_i^(n) ;
                    Compute power level p_i^(n) from (3.15) ;
                end
            end
        end
    end
until end of iteration;
```

Remark 3.2. The general setting considered here is also applicable to cognitive radio systems, where individual mobiles have the ability to sense their environment, and act strategically as independent decision makers[82]. While allocating power it is made sure that the receiver SINR from each primary user to the base station is kept above

a minimum level by limiting the interference caused by the secondary users. Here, the primary base station can act as the designer and employ pricing mechanisms to align power selection decisions so as to achieve a global objective.

3.2.3 Numerical Simulation

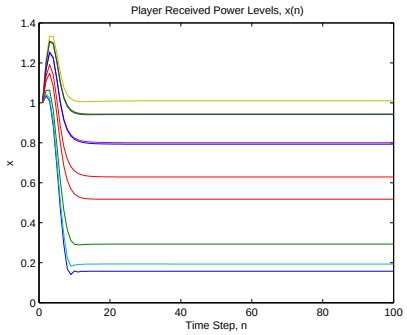

Figure 3.2: The evolution of user power levels $\mathbf{x}$ in pricing mechanism $\mathscr{M}_a$ for a single carrier.

First, numerical simulation results are presented for the case, $U_i(\mathbf{x}) = \rho_i \sum_n \log(\gamma_i^{(n)}),\ \forall\, i$, to establish the efficiency and convergence of the proposed mechanisms. The iterative pricing mechanism for social welfare maximization for multi carrier systems is illustrated numerically. We simulate this scenario with 10 users and the following arbitrarily chosen utility parameters

$$\rho = [0.23\ , 1.33\ , 0.73\ , 0.28\ , 1.13\ , 1.65\ , 1.35\ , 2.00\ , 1.92\ , 0.12].$$

The users update their power levels according to (3.15) at each time step $k \geq 1$ with a step size of $\kappa_i = 0.2, \forall i$. The designer, on the other hand, updates the Lagrangian

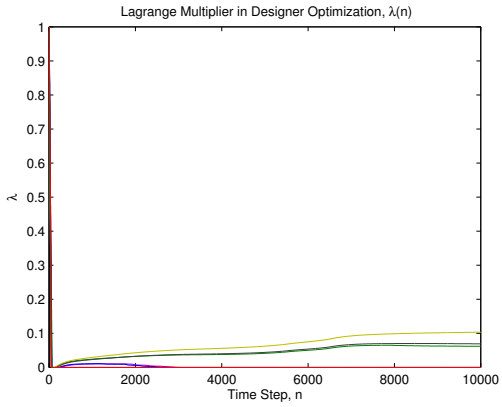

Figure 3.3: The evolution of Lagrange multiplier λ in pricing mechanism $\mathscr{M}_a$ for a single carrier.

multipliers λ's and price vector $\mathbf{P}$ based on (3.16) and (3.14), where $X_{max} = 1$ and $\kappa_D = 0.5$. The background noise parameter is $\sigma = 0.5$.

The convergence of the mechanism $\mathscr{M}_a$ is depicted in Figures 3.2 and 3.3.

The power levels for multi carrier system with number of carriers $M = 5$ and number of users $N = 10$ are plotted in Figure 3.4. The other parameters are same as above. For demonstration purpose the curves are shown for 3 users.

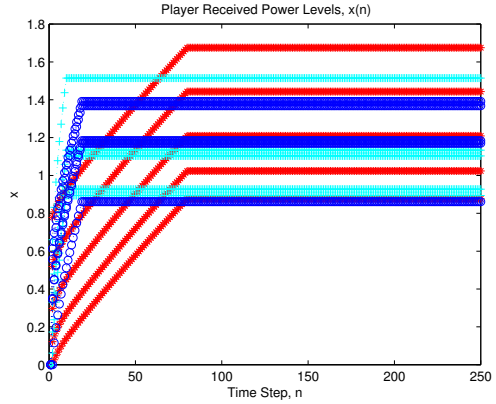

Figure 3.4: The evolution of user power levels $\mathbf{x}$ in pricing mechanism for multiple carriers.

3.3 Revenue Maximization in Wireless Networks

In this section, we consider a scenario in which in addition to pricing user transmit powers for obtaining social goals, the designer may like to maximize the revenue obtained from

these prices.

3.3.1 Revenue Maximization Mechanism

We next introduce pricing mechanisms for designer **revenue maximization** which may lead to non optimal social welfare. There are optimal auctions introduced by Myerson [86] in which the designer knowing the distribution of private values of players maximizes the expected revenue. In [45], revenue maximization of the operator is considered and an iterative algorithm is proposed for single carrier systems. The users are charged for the throughput they obtain in which the prices are not functions of the Lagrange multipliers.

In this section, the global objective of the designer aims to maximize her total revenue as a monopolistic entity, while trying to limit the user power levels to X_{max}. The total revenue of the designer will be,

$$V(\mathbf{x}) = \sum_j \sum_n P_j^{(n)}(x) x_j^{(n)}.$$

The designer D solves the constrained optimization problem

$$\max_{\mathbf{x}} \sum_j \sum_n P_j^{(n)}(x) x_j^{(n)} \text{ such that } \sum_n \frac{x_i^{(n)}}{h_i^{(n)}} \leq X_{max} \ \forall i, n, \text{and} \sum_j \sum_n \frac{x_j^{(n)}}{h_j^{(n)}} \leq X_{total}.$$

As in previous case, we obtain a matrix form solution for optimal prices. Also an iterative method which uses Lagrangian multipliers can give the prices and powers. Next section gives the numerically obtained power levels and value of λ which maximizes revenue.

3.3.2 Numerical Simulation

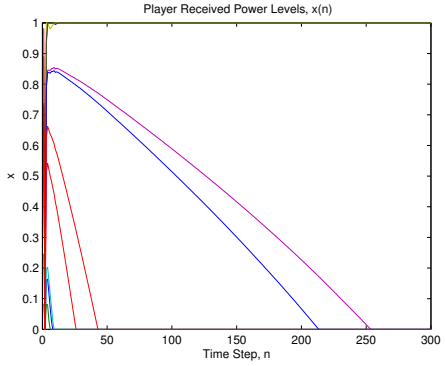

Figure 3.5: The evolution of user power levels $\mathbf{x}$ in pricing mechanism $\mathscr{M}_d$ for revenue maximization.

For the revenue maximizing mechanism, the convergence of power levels and lambda levels are plotted in Figures 3.5 and 3.6. A boundary solution behavior is observed as

similar to efficiency maximizing mechanisms, but with different number of users touching the power constraint.

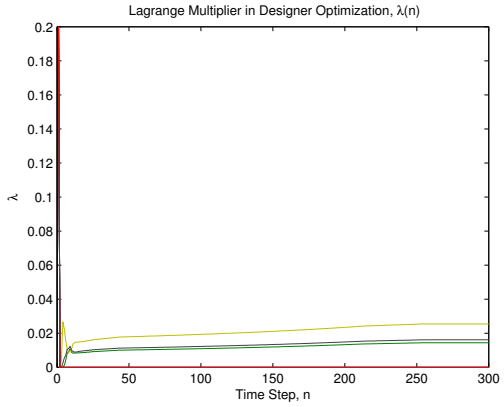

Figure 3.6: The evolution of Lagrange multiplier λ in pricing mechanism $\mathscr{M}_d$ for revenue maximization.

3.4 Energy Minimization in Networks

3.4.1 Introduction

There has been significant amount of work in the context of Ad-hoc [46] and sensor networks [81] to obtain energy efficient protocols. In game theoretic model is proposed for energy efficient power control by defining utility of users as the ratio of throughput (goodput) and power (with unit bit/J) We note that most of the previous works on game models for energy efficiency modify user utilities by incorporating a power term into the user utility function[79, 78, 16], assuming that users care for their energy usage in uplink transmission. In contrast, we consider here the alternative scenario and assume that the users care only for getting maximum throughput, but an external mechanism designer imposes prices to the users such that their energy consumption is decreased to improve overall energy efficiency of the system. Thus, the designer encourages users to be more energy conscious. In addition, we also consider user utility dependence on higher layer parameters.

We model energy efficiency objective by subtracting a *general convex function of the power levels* of users from the social welfare (sum of utilities of all users). This additional term is multiplied by a tuning parameter which allows smoothly varying the emphasis from the social welfare to the system energy efficiency. The energy efficiency objective is,

$$V(\mathbf{x}) = \sum_i U_i(\mathbf{x}) - \phi R(\mathbf{x}). \tag{3.19}$$

where $0 \leq \phi \leq 1$ is the tuning parameter and $R(x)$ is any convex function on x that captures the cost on energy usage. It is similar to cost of control in other settings. Due to the convexity of the additional term, we can see that the users sacrifice much on their net utility if they transmit with higher power. A specific example function is, $R(\mathbf{x}) = \sum_i R_i(x_i)$, where $R_i(x_i)$ can be any convex function of x_i. The underlying game of the mechanism converges to a Nash equilibrium iteratively in a way that the users respond to the prices set by the designer.

3.4.2 Energy Efficient Mechanism

In pricing mechanisms, the designer charges the players for their resource usage and players take actions in response to that. Pricing mechanisms are applicable to many networked systems where an explicit allocation of resources brings a prohibitively expensive overhead or simply not feasible, e.g. due to participating players being selfish or located in a distributed manner.

The global objective of designer with individual user power constraint is to solve the optimization,

$$\max_x \sum_i U_i(\mathbf{x}) - \phi \sum_i R_i(x_i) \text{ such that } \sum_n \frac{x_i^{(n)}}{h_i^{(n)}} \leq X_{max},$$

where X_{max} is the maximum allowable power to individual users. The constraint on the maximum allowable power level will be set by the regulating authority due to the limit on total interference. The designer, apart from this requirement, is concerned about the total energy consumption in the cell. The nature of the designer, i.e, the extend to which she cares about energy efficiency, is captured in the parameter ϕ. Thus, the Lagrangian function of the designer problem can be written as:

$$\begin{aligned} L &= U_i(\mathbf{x}) + \sum_{j \neq i} U_j(x) - \phi \sum_i R_i(x_i) \\ &- \sum_i \lambda_i (\sum_n \frac{x_i^{(n)}}{h_i^{(n)}} - X_{max}), \end{aligned} \tag{3.20}$$

where λ_i's are the Lagrangian multipliers.

This problem can be solved by convexification as described in [26]. The corresponding Karush-Kuhn-Tucker (KKT) conditions are:

$$\frac{dU_i}{dx_i^{(n)}} + \sum_{j \neq i} \frac{dU_j(x)}{dx_i^{(n)}} - \phi \frac{dR_i}{dx_i^{(n)}} - \frac{\lambda_i}{h_i^{(n)}} = 0, \forall\ i, n,$$

$$\lambda_i (\sum_n \frac{x_i^{(n)}}{h_i^{(n)}} - X_{max}) = 0.$$

We next align the solution of both designer and user problems, and obtain the price and action vectors that solve all of them concurrently. By combining the above KKT

conditions and the conditions of user best response from equation (3.5) in the previous section, we obtain the prices as:

$$P_i^{(n)} = \phi \frac{dR_i}{dx_i^{(n)}} - \sum_{j \neq i} \frac{dU_j(x)}{dx_i^n} + \frac{\lambda_i}{h_i^{(n)}} \ \forall i, n. \tag{3.21}$$

Consider for demonstration purpose that the users have their utility as total Shannon capacity over all the channels in high SIR region, i.e.,

$$U_i(\mathbf{x}) = \rho_i \sum_n \log(\gamma_i^{(n)}(\mathbf{x}))$$

where ρ is user preference vector unknown to the base station and energy cost term as

$$R_i(x_i) = \frac{\sum_n (p_i^{(n)})^2}{2} = \frac{1}{2} \sum_n \frac{(x_i^{(n)})^2}{(h_i^{(n)})^2}.$$

Notice that due to the weighting by channel coefficients, good channels are encouraged in this case while bad ones are discouraged. Then,

$$\frac{dU_i}{dx_i^n} = \frac{\rho_i}{x_i^n} = P_i^{(n)}, \tag{3.22}$$

and

$$\frac{dU_j}{dx_i^n} = \frac{-\rho_j}{(\sum_{k \neq j} x_j^{(n)} + \sigma)}.$$

In this special case, the prices from (3.21) can be written as

$$P_i^{(n)} = \phi \frac{x_i^{(n)}}{(h_i^{(n)})^2} + \sum_{j \neq i} \frac{\rho_j}{(\sum_{k \neq j} x_j^{(n)} + \sigma)} + \frac{\lambda_i}{h_i^{(n)}} \ \forall i, n. \tag{3.23}$$

Using (3.22) and definition of γ_j^n,

$$P_i^{(n)} = \sum_{j \neq i} \gamma_j^n P_j^n + \phi \frac{x_i^{(n)}}{(h_i^{(n)})^2} + \frac{\lambda_i}{h_i^{(n)}}, \ \forall i, n. \tag{3.24}$$

The above set of equations can also be written in matrix form like in the social welfare maximization case as,

$$A^{(n)} \cdot P^{(n)} = B^{(n)} \cdot L^{(n)}, \ \forall n,$$

where the matrices $A^{(n)}$ and $B^{(n)}$ are defined as

$$A^{(n)} := \begin{pmatrix} 1 & -\gamma_2^{(n)} & \cdots & -\gamma_N^{(n)} \\ -\gamma_1^{(n)} & 1 & \cdots & -\gamma_N^{(n)} \\ \vdots & & \ddots & \vdots \\ -\gamma_1^{(n)} & -\gamma_2^{(n)} & \cdots & 1 \end{pmatrix}, \tag{3.25}$$

$$B^{(n)} := \begin{pmatrix} \frac{1}{h_1^{(n)}} & \cdots & 0 & \frac{\phi}{(h_1^{(n)})^2} & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots & \vdots & \\ 0 & \cdots & \frac{1}{h_N^{(n)}} & 0 & \cdots & \frac{\phi}{(h_N^{(n)})^2} \end{pmatrix}$$

and $L^{(n)} = [\lambda_1, \ldots, \lambda_N, x_1^{(n)}, \ldots, x_N^{(n)}]^T$.

3.5 Pricing Games in Multihop Wireless Networks under Interference Constraints

3.5.1 Introduction

In this section, we consider joint power and rate allocation in multihop wireless networks. We consider a wireless network scenario where an MBS (Source) uses multiple relay nodes owned by some second parties to give better service to the MUs. A specific instance of the problem is given in Figure 3.7, with an MBS, two relays and an MU. The MU at the cell edge is better served using the two relays, an FBS and a PBS, which are rewarded by the MBS for forwarding the traffic to the MU. The practical scenario we consider is one in which the Femto or Pico cells are used as relays by their owners to get additional revenue apart from self usage. In this wireless network setting, selfish and strategic relays

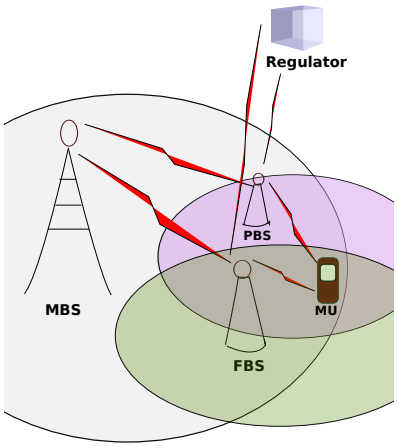

Figure 3.7: A Pico Base Station (PBS) and a Femto Base Station (FBS) acting as relays for the Macro Base Station (MBS) to give service to user at the cell edge.

engage in a game where each relay strategize on the charging function they submit to the source, as well as the transmission power to the end user. The transmissions on different wireless links in this multihop network interfere with each other, with the link

capacities dependent on the power allocation on all links. Each relay designs its best response based on its cost, according to the traffic flow rate and transmission power allocated by the source, as well as the charging functions and power selections of the other relays. We examine the Nash Equilibria (NE) which result from this game, which may not yield an efficient resource allocation from a social welfare standpoint. We use the Price of Anarchy (PoA)[65] as the metric to characterize the inefficiency of the resource allocation at the NE, as compared with the socially optimal allocation.

Within the game setting discussed above, we introduce the concept of *interference tax* which the relays should pay to an external regulator as compensation for the interference they create to other relays. We prove that inefficient NE occur when the price is a function only of the traffic flow rate through the relays. On the other hand, we prove that there exists at least one NE which is efficient when the charging function depends on both the traffic flow rate and the transmission powers from the relays to the destination. Our result highlights the importance of interference coupling among the relays in determining network resource allocation in a selfish and strategic context.

3.5.2 Game Model for Multihop Wireless Networks

We consider a network in which a Source transmits to a destination through $\{1, \cdots, i, \cdots N\}$ parallel relays. The model is depicted in Figure 3.8. The cost on link (s, i) from Source s to relay i, denoted by J_{si}, is the sum of two components: the congestion cost D_{si} and the power cost $\alpha_s x_{si}$. The congestion cost D_{si} is a function of the capacity C_{si} of link (s, i), and the traffic flow rate F_i on link (s, i). The power cost $\alpha_s x_{si}$ consists of the balancing parameter $\alpha_s \in \Re^+$ and the transmission power x_{si} from Source s to relay i.

Unlike the case for wireline networks, the capacity of a wireless link is not fixed, but rather depends on the channel conditions and the transmission powers. The joint power and rate allocation for the links from the Source to the relays is carried out by the Source.

For the case of spread spectrum CDMA, the Shannon capacity C_{si} is given by

$$C_{si}(\mathbf{x}_s) = \frac{R_s}{2} \log \left(1 + \frac{K h_{si} x_{si}}{\sum_{j \neq i} h_{sj} x_{sj} + \sigma} \right),$$

where $\mathbf{x}_s \equiv (x_{s1}, \ldots, x_{sN})$, h_{si} is the channel gain from Source s to relay i, R_s is the symbol rate, K is the code gain, and σ is the noise power at the receiver of i. Since the code gain K is typically high, we assume that the operation is in the high SINR regime, where the capacity can be approximated by

$$C_{si}(\mathbf{x}_s) \approx \frac{R_s}{2} \log \left(\frac{K h_{si} x_{si}}{\sum_{j \neq i} h_{sj} x_{sj} + \sigma} \right). \tag{3.26}$$

This approximation, along with the following assumption, facilitates the convexification of the optimization problems arising later in this chapter.

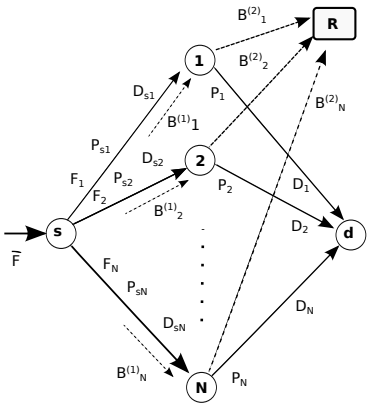

Figure 3.8: Multihop wireless network model with N relays. F_i is the flow rate on link i; x_{si} is the transmission power from Source s to relay i; x_i is the transmission power from relay i to destination d; D_{si} is the congestion cost from s to i; D_i is the congestion cost from i to d; $B_i^{(1)}$ is the payment paid by s to relay i; Regulator R receives the payments $B_i^{(2)}$ from the relays.

Assumption 3.1. *The congestion cost $D_{si}(C_{si}, F_i)$ is a twice differentiable, convex and increasing function of F_i, and a twice differentiable, convex and decreasing function of C_{si}.*

Let the payment made by the Source to the relay i be B_i. As discussed below, B_i can be a function of the flow rate F_i carried by relay i, as well as other variables. Thus, the Source incurs the total cost

$$J_s(\mathbf{x}_s, \mathbf{F}) = \sum_{i=1}^{N} \left[D_{si}(C_{si}(\mathbf{x}_s), F_i) + \alpha_s x_{si} + B_i \right]. \tag{3.27}$$

We assume that the source-to-relay communication channel is orthogonal to the relay-to-destination communication channel. Let $\mathbf{x} \equiv (x_1, \ldots, x_N)$, where x_i is the transmission power from relay i to the destination. The capacity of the wireless link from relay i to the destination is approximated by

$$C_i(\mathbf{x}) \approx \frac{R_s}{2} \log \left(\frac{K h_i x_i}{\sum_{j \neq i} h_j x_j + \sigma} \right),$$

where h_i is the channel gain from relay i to the destination, and σ is the noise power at the destination receiver. Therefore, each relay i has a total cost of transmission J_i to

the destination, given by

$$J_i(\mathbf{x}, F_i) = D_i(C_i(\mathbf{x}), F_i) + \alpha_i x_i - B_i. \tag{3.28}$$

where D_i satisfies Assumption 3.1 and α_i is a balancing parameter. Note that the total cost over parallel path i is given by

$$D_{si}(C_{si}(\mathbf{x}_s), F_i) + D_i(C_i(\mathbf{x}), F_i) + \alpha_s x_{si} + \alpha_i x_i. \tag{3.29}$$

The power allocation from the Source to the relays is accomplished centrally at the Source, whereas the transmission powers from the relays to the destination are selected in a distributed manner by the relays. Each relay i competes with all other relays by selecting the payment function B_i and transmission power x_i, in order to maximize its net profit, which is equal to the revenue generated by forwarding a share of the traffic from the Source to the destination, minus the power expense required for forwarding the traffic. This is the basis of the game among the relays.

All relays should gain positive net utility by participating in the game, a condition usually known as the Individual Rationality (IR) property [38]. The IR constraint in the relay problem is given by: $J_i(x_i) \leq 0$ for all $i = 1, \ldots, N$. The IR constraint is satisfied through the following process. First, the relays submit charging functions. Then, the source decides on the optimal flows in response to these payment functions, without taking into account the IR constraint on each relay. Given this, some relays may find that they cannot find a positive finite power which will ensure negative cost, for the flow given by the source and power chosen by other relays. This might happen, for instance, if the channel gains from those relays to the destination are very low compared to others. In this case, these relays will opt out of the game and will report this to the source. Subsequently, the source will reallocate its flows excluding the non-participating relays. This process continues until a stable subset of relays satisfying the IR constraint emerges.

3.5.3 Pricing Function for Efficient NE in Multihop Wireless Networks

The aggregate network cost is the sum of the costs on all parallel paths. Therefore, the global optimization for obtaining the socially optimal (efficient) operating point is given by

$$\min_{\mathbf{x}_s, \mathbf{x}, \mathbf{F}} \sum_{i=1}^{N} [D_{si}(C_{si}(\mathbf{x}_s), F_i) + \alpha_s x_{si} + D_i(C_i(\mathbf{x}), F_i) + \alpha_i x_i]$$
$$\text{s.t.} \sum_i F_i = \overline{F}, F_i \geq 0, x_i \geq 0, x_{si} \geq 0, \forall i. \tag{3.30}$$

This problem can be shown to be jointly convex in the log power variables $\mathbf{S}_s = \log(\mathbf{x}_s)$, $\mathbf{S} = \log(\mathbf{x})$, and the flow vector $\mathbf{F}$ using the high SINR assumption and Assumption 3.1.

After the log transformation, the global optimization becomes

$$\min_{\mathbf{S}_s,\mathbf{S},\mathbf{F}} \sum_{i=1}^{N} \left[D_{si}(C_{si}(\mathbf{S}_s), F_i) + \alpha_s e^{S_{si}} + D_i(C_i(\mathbf{S}), F_i) + \alpha_i e^{S_i}\right]$$
$$\text{s.t.} \sum_i F_i = \overline{F}, F_i \geq 0, \ \forall\ i. \tag{3.31}$$

The above problem leads to the following KKT conditions for global optimality. For each $i = 1, \ldots, N$,

$$\frac{\partial D_{si}}{\partial F_i} + \frac{\partial D_i}{\partial F_i}\Big|_{\mathbf{F}=\mathbf{F}^g} = d^g \text{ if } F_i^g > 0,$$
$$\frac{\partial D_{si}}{\partial F_i} + \frac{\partial D_i}{\partial F_i}\Big|_{\mathbf{F}=\mathbf{F}^g} > d^g \text{ if } F_i^g = 0, \tag{3.32}$$
$$\frac{\partial D_{si}}{\partial S_{si}} + \sum_{j\neq i} \frac{\partial D_{sj}}{\partial S_{si}} + \alpha_s e^{S_{si}}\Big|_{\mathbf{S}_s=\mathbf{S}_s^g} = 0, \tag{3.33}$$
$$\frac{\partial D_i}{\partial S_i} + \sum_{j\neq i} \frac{\partial D_j}{\partial S_i} + \alpha_i e^{S_i}\Big|_{\mathbf{S}=\mathbf{S}^g} = 0, \tag{3.34}$$

where $\mathbf{x}_s^g, \mathbf{x}^g, \mathbf{F}^g$ are the globally optimal source transmission power vector, relay transmission power vector, and flow rate vector, respectively, and d^g is a constant which corresponds to the optimal operating point. We analyze the pricing game in which the relays compete with each other for the traffic allocation from the Source by strategizing on the charging function and the power of transmission to the destination. Each relay sends a charging function B_i to the Source, which performs the flow allocation and power allocation to the relays according to the charging function.

As a first step, as in [117], we assume that the Source is charged as a function of the flow rates it sends through the relays, i.e., the charging functions are given by $B_i(F_i)$. The Source optimization problem is to minimize the cost given by (3.27), i.e.,

$$\min_{\mathbf{x}_s,\mathbf{F}} \sum_i (D_{si}(C_{si}(\mathbf{x}_s), F_i) + \alpha_s x_{si} + B_i(F_i)), \tag{3.35}$$
$$\text{s.t.} \sum_i F_i = \overline{F}, F_i \geq 0 \ \forall i \text{ and } x_{si} \geq 0 \ \forall\ i$$

The Source decides on the flow and power vectors on each link to the relays by solving the above problem for every set of charging functions given by the relays. This problem can be shown to be jointly convex in high SINR region, in the log power variables $\mathbf{S}_s = \log(\mathbf{x}_s)$ and the flow vectors $\mathbf{F}$ if the payment is a convex function of the flow. The

Source KKT conditions are:

$$\begin{aligned} \frac{\partial D_{si}}{\partial F_i} + \frac{\partial B_i}{\partial F_i}\Big|_{\mathbf{F}=\mathbf{F}^*} = d^* \text{ if } F_i^* &> 0, \\ \frac{\partial D_{si}}{\partial F_i} + \frac{\partial B_i}{\partial F_i}\Big|_{\mathbf{F}=\mathbf{F}^*} > d^* \text{ if } F_i^* &= 0,\ \forall i \qquad (3.36) \\ \frac{\partial D_{si}}{\partial S_{si}} + \sum_{j\neq i} \frac{\partial D_{sj}}{\partial S_{si}} + \alpha_s e^{S_{si}}\Big|_{\mathbf{S}_s=\mathbf{S}_s^*} &= 0, \forall i \qquad (3.37) \end{aligned}$$

where $\mathbf{x}_s^* = e^{\mathbf{S}_s^*}$ and $\mathbf{F}^*$ give the solution of the Source optimization and d^* corresponds to the Source optimal operating point.

In the associated game, relays strategize using the charging functions, $\mathbf{B}$, and the transmission power to the end user, $\mathbf{x}$. The relays are implicitly competing over the transmission powers due to the interference they cause to each other. The relays also compete for the traffic flow using the payment they charge from the Source. Due to the coupling in the cost term $D_i(C_i(\mathbf{x}), \mathbf{F}_i)$, we can think of the relays as deciding on the charging function and the transmission powers at the same time. The strategy space of each relay is infinite dimensional in general.

The NE of this game can be obtained from the intersection of the best responses of all relays, given by

$$(\mathbf{S}_i^*, \mathbf{B}_i^*) \in \arg\min_{S_i, B_i} J_i(S_i, B_i, \mathbf{S}_{-i}, \mathbf{B}_{-i}),\ \forall\ i. \qquad (3.38)$$

Definition 3.2. A NE is efficient if the flow rate allocation and power allocation at the NE solves the global optimization.

In the multihop wireless problem we consider, an NE is efficient when $\mathbf{S}^* = \mathbf{S}^g, \mathbf{F}^* = \mathbf{F}^g, \mathbf{S}_s^* = \mathbf{S}_s^g$, where $(\mathbf{S}_s^*, \mathbf{F}^*)$ is the solution to the source optimization problem when the relays present the NE charging functions $\mathbf{B}^*$ from (3.38) to the Source. The following Proposition shows that this situation cannot obtain when the charging function depends only on the traffic flow rate.

Proposition 3.3. *A Nash Equilibrium of the pricing game cannot be efficient when the relay charging functions depend only on the traffic flow rate carried by the relays.*

Proof. Suppose that there exists an efficient Nash equilibrium $\mathbf{S}^*, \mathbf{B}^*$ with the charging function $B_i(F_i)$. The Source solves the following optimization problem to find the Source optimal power and flow

$$(\mathbf{S}_s^*, \mathbf{F}^*) = \arg\min_{\mathbf{S}_s, \mathbf{F}} \sum_i (D_{si}(C_{si}(\mathbf{S}_s), F_i) + \alpha_s e^{S_{si}} + B_i^*(F_i))$$
$$\text{s.t.} \sum_i F_i = \overline{F},\ F_i \geq 0\ \forall i$$

This results in the following KKT conditions.

$$\begin{aligned} \frac{\partial D_{si}}{\partial F_i} + \frac{\partial B_i^*}{\partial F_i}\Big|_{\mathbf{F}=\mathbf{F}^*} = d^* \text{ if } F_i^* &> 0, \\ \frac{\partial D_{si}}{\partial F_i} + \frac{\partial B_i^*}{\partial F_i}\Big|_{\mathbf{F}=\mathbf{F}^*} > d^* \text{ if } F_i^* &= 0, \ \forall i \end{aligned} \tag{3.39}$$

$$\frac{\partial D_{si}}{\partial S_{si}} + \sum_{j\neq i} \frac{\partial D_{sj}}{\partial S_{si}} + \alpha_s e^{S_{si}}\Big|_{\mathbf{S}_s=\mathbf{S}_s^*} = 0, \forall i \tag{3.40}$$

Once the relays receive the allocation $\mathbf{S}_s^*, \mathbf{F}^*$ from the Source, they minimizes the relay cost in equation (3.28) to find the best response.

$$\mathbf{S}_i^* = \arg\min_{\mathbf{S}_i} D_i(C_i(S_i, \mathbf{S}_{-i}^*), F_i^*) + \alpha_i e^{S_i} - B_i^*(F_i^*) \ \forall i. \tag{3.41}$$

The KKT conditions for the relay optimization w.r.t. $\mathbf{S}$ which give the NE $\mathbf{S}^*$ are:

$$\frac{\partial D_i(C_i(S_i, \mathbf{S}_{-i}^*), F_i^*)}{\partial S_i} + \alpha_i e^{S_i}\Big|_{\mathbf{S}=\mathbf{S}^*} = 0, \forall i \tag{3.42}$$

From the Definition 3.2, for the NE point to be efficient, the solution of (3.32) (3.33) and (3.34) and the joint solution of (3.39),(3.40), and (3.42) should be the same. We observe that it is not enough to set

$$\frac{\partial B_i^*}{\partial F_i}\Big|_{\mathbf{F}=\mathbf{F}^*} = \frac{\partial D_i}{\partial F_i}\Big|_{\mathbf{F}=\mathbf{F}^g}, \ \forall i$$

as in [117]. Indeed, we can see from the KKT conditions w.r.t. $\mathbf{S}$ in (3.34) and (3.42), that the resulting solutions are different, as the second (interference) term in (3.34) is not accounted for in (3.42). Therefore, the KKT conditions of the NE solution and globally optimal solution are not aligned. In general, $\mathbf{S}^* \neq \mathbf{S}^g, \mathbf{F}^* \neq \mathbf{F}^g, \mathbf{S}_s^* \neq \mathbf{S}_s^g$ and the NE cannot be efficient. □

We now consider an alternative approach. Assume that the charging function depends on both the traffic flow rate forwarded by the relay and the power the relay spends for the relaying, i.e. $B_i(F_i, x_i)$. Specifically, we split the charging function as follows: $B_i(F_i, x_i) = B_i^{(1)}(F_i) - B_i^{(2)}(x_i)$. The payment $B_i^{(1)}(F_i)$ is paid by the Source to the relay, while the payment $B_i^{(2)}(x_i)$ is paid by the relay to a centralized controller.

Theorem 3.4. *There exists an efficient NE in the pricing game where the charging function is given by $B_i(F_i, S_i) = B_i^{(1)}(F_i) - B_i^{(2)}(S_i)$, satisfying*

$$\frac{\partial B_i^{(1)*}}{\partial F_i}\Big|_{\boldsymbol{F}=\boldsymbol{F}^*} = \frac{\partial D_i(\boldsymbol{x}, F_i)}{\partial F_i}\Big|_{\boldsymbol{F}=\boldsymbol{F}^g}, \forall i \tag{3.43}$$

and

$$\frac{\partial B_i^{(2)*}}{\partial S_i}\Big|_{\boldsymbol{S}=\boldsymbol{S}^*} = \sum_{j\neq i} \frac{\partial D_j(\boldsymbol{x}, F_j)}{\partial S_i}\Big|_{\boldsymbol{S}=\boldsymbol{S}^g}, \forall i. \tag{3.44}$$

where $(\boldsymbol{S}^*, B^{(1)*}, B^{(2)*}, \boldsymbol{F}^*)$ is the NE and $(\boldsymbol{S}^g, \boldsymbol{F}^g)$ is the global optimum.

Proof. A standard result in game theory (Theorem 4.4, p.176, in [13]) for convex cost functions which satisfy Assumptions 3.1, proves that the game we consider admits a NE.

Given the payment charge $B^{(1)*}(F_i)$ from the relays, the Source cost becomes

$$J_s = \sum_i (D_{si}(C_{si}(\mathbf{S}_s), F_i) + \alpha_s e^{S_{si}} + B_i^{(1)*}(F_i)). \tag{3.45}$$

The KKT conditions for Source optimization are

$$\begin{aligned}
\frac{\partial D_{si}}{\partial F_i} + \frac{\partial B_i^{(1)*}}{\partial F_i}\Big|_{\mathbf{F}=\mathbf{F}^*} = d^* \text{ if } F_i^* &> 0, \\
\frac{\partial D_{si}}{\partial F_i} + \frac{\partial B_i^{(1)*}}{\partial F_i}\Big|_{\mathbf{F}=\mathbf{F}^*} > d^* \text{ if } F_i^* &= 0, \ \forall i \qquad (3.46) \\
\frac{\partial D_{si}}{\partial S_{si}} + \sum_{j\neq i} \frac{\partial D_{sj}}{\partial S_{si}} + \alpha_s e^{S_{si}}\Big|_{\mathbf{S}_s=\mathbf{S}_s^*} &= 0, \forall i \qquad (3.47)
\end{aligned}$$

where $\mathbf{F}^*, \mathbf{S}_s^*$ is the source-optimal solution. With this allocation from the Source, the relays carry out their optimizations

$$S_i^* = \arg\min_{S_i} \qquad D_i(C_i, F_i) + \alpha_i e^{S_{si}} - B_i^{(1)*}(F_i) + B_i^{(2)*}(S_i), \ \forall i. \tag{3.48}$$

The KKT condition for relay optimization is,

$$\frac{\partial D_i}{\partial S_i} + \alpha_i e^{S_i} + \frac{\partial B_i^{(2)*}}{\partial S_i}\Big|_{S_i=S_i^*} = 0, \forall i \tag{3.49}$$

In order to obtain an efficient NE, from (3.32) and (3.46), we obtain the condition in (3.43). From (3.34) and (3.49), we obtain the condition in (3.44). □

The relays receive payments from the Source for the traffic flow they carry, and are charged for the interference they create to other relays. We introduce an outside regulator which collects the *interference tax* payments from the relays. As an instance of the pricing given in (3.44), we propose logarithmic pricing on power for the interference tax. The logarithmic pricing is also similar to the universal pricing proposed in [19] for a different setting other than multihop wireless networks and without flow variables. The authors in [19] show that logarithmic pricing in power is universal pricing for systems with certain class of interference coupled utility functions. We set

$$B_i(F_i, x_i) = a_i F_i - b_i \log(x_i).$$

According to (3.43) and (3.44), the coefficients are given by,

$$a_i = \frac{\partial D_i}{\partial F_i}\Big|_{\mathbf{F}=\mathbf{F}^g}, \ \forall \ i \tag{3.50}$$

and

$$b_i = \sum_{j\neq i} \frac{\partial D_j}{\partial S_i}\Big|_{\mathbf{S}=\mathbf{S}^g}, \ \forall \ i. \tag{3.51}$$

Note that due to the high SINR assumption, $x_i > 1$ for any relay i, and the logarithmic power price is positive.

3.5.4 *PoA* When Price is a Function Only of the Flow

We now examine the inefficiency of the NE when the charging function is a function only of the traffic flow rate through the link.

The Price of Anarchy (PoA) in a multihop network at an NE denoted by $(\mathbf{x}_s^*, \mathbf{x}^*, \mathbf{B}^*, \mathbf{F}^*)$ is obtained from Definition 2.16 as

$$PoA = \frac{J_g(\mathbf{x}_s^*, \mathbf{x}^*, \mathbf{F}^*)}{J_g(\mathbf{x}_s^g, \mathbf{x}^g, \mathbf{F}^g)}$$

where J_g denotes the global cost and $(\mathbf{x}_s^g, \mathbf{x}^g, \mathbf{F}^g)$ is the globally optimal solution.

For interference coupled systems, we have observed that efficiency loss results when the charging function is a function only of the traffic flow rate, as in the case of [117]. We now consider a two-relay example with charging functions which depend linearly on the traffic flow rate, i.e. $B_i(F_i) = a_i F_i$, where a_i is given by (3.50). In this case, $x_{s1}^*, x_{s2}^*, F_1^*$ are obtained from (3.39) and (3.40), while x_1^*, x_2^* result from the following relay KKT conditions:

$$\frac{\partial D_1(\mathbf{S}, F_1^*)}{\partial S_1} + \alpha_1 S_1 \Big|_{S_1 = S_1^*} = 0, \tag{3.52}$$

$$\frac{\partial D_2(\mathbf{S}, F_1^*)}{\partial S_2} + \alpha_2 S_2 \Big|_{S_2 = S_2^*} = 0. \tag{3.53}$$

Since it is not easy to solve these equations analytically, we solve the equations numerically. The resulting PoA is plotted in the next section.

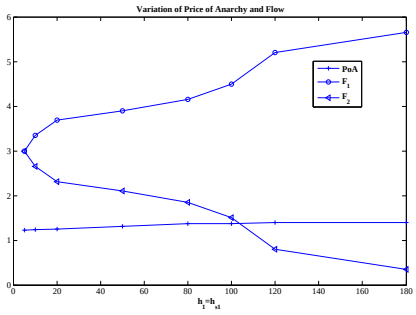

Figure 3.9: The PoA and path flows as functions of the channel gain in path 1.

3.5.5 Numerical Simulation

We numerically simulate the range of values of PoA for the two-relay example described in previous section. The $\overline{F}$ parameter is fixed at 6. First, the values a_1 and a_2 are selected as the marginal cost w.r.t. to the flows at the globally optimal point. Then, the source optimization problem is solved using a_1 and a_2 to find the flow and source power vector at the NE point. At the values of F_1 and F_2 given by the source optimum, the NE power vectors are found by the relays individually. The power vectors are different from the global point and give rise to PoA values as shown in Figure 7.2. The channel parameters $h_{s2} = h_2$ are set to 5. The parameters h_1 and h_{s1} are varied from 5 to 180. We stop at $h_1 = h_{s1} = 180$ since it is observed that after 180 the link from Relay 2 to the destination cannot have positive capacity, and due to the IR constraint, Relay 2 opts out from the game. The optimal flow allocation at the NE is also shown in Figure 7.2. As the link to relay 1 has higher channel gain compared to the link to relay 2, there is

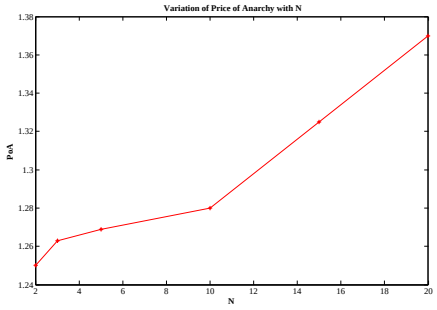

Figure 3.10: The variation of PoA with the number of relays N.

more flow allocated to relay 1. We can observe that the PoA increases as the channel gains become dissimilar. In the asymmetric case, when the Source finds the optimal flow, it does not take into account the asymmetry of the channel gains from relays to the destination, since the price is only a function of the flow. On the other hand, the global allocation is affected by the asymmetry of the channel gains from relays to the destination. For this reason, there is a higher PoA when the channel gains from the relays to the destination are asymmetric. This is numerically shown in Figure 7.2.

Finally, we show the variation of PoA with the number of relays N in Figure 3.10. The parameters are selected as above with $h_{s1} = h_1 = 20$ and $h_{s2} = h_2 = 5$, with the number of relays varying up to 20. We can see that the PoA increases as the number of relays increases.

3.6 Concluding Remarks

In this chapter, first pricing functions have been derived based on three global objectives of the designer for an MC-CDMA system. The prices can be implemented with minimum communication requirement since the designer needs to only calculate the Lagrange multipliers of different constraints and measure the received SINR vector. An iterative algorithm is also proposed of the implementation whose convergence is analytically dealt in Chapter 5. For multihop network with Femto cell relays, the relays are made to pay *interference tax* from the incenive which they get in proportional to the traffic they carry to an external regulator. It has been observed that the PoA when price is only a function of flow is higher in asymmetric networks.

4 Location Privacy Mechanism for Mobile Commerce with Entropy Utility Functions

4.1 Introduction

In this chapter, we apply the pricing mechanism which was proposed in the previous chapter in a location privacy problem, with proper modifications. We consider a mobile commerce environment in which the users or customers get benefits from a company (service provider) by disclosing their location with certain degree of accuracy. At the same time, disclosing their location information brings users certain risks and compromises their privacy. Therefore, users have a motivation to maintain anonymity by giving less granular information about their location or no information at all.

In [74], a game theoretic model of privacy in a community-based social networking mobile applications is proposed, in which the users take decisions on the level of granularity with which they share their location information to others. In that model, there is no service provider and the individual members of the community use their collective knowledge for personal or social goals. A Pareto improvement of the Nash equilibrium is also achieved by making the users to contribute more information to the collective knowledge, using a tit-for-tat mechanism. In this chapter, we propose a *mechanism design* [72] approach in which the company acts as a designer and properly motivates its users through the benefits in terms of payment[109] provided to them, in order to obtain desired *granularity of location information* from all the users. We refer to the mechanisms in this setting as *privacy mechanisms*.

The benefits offered by the company to the users can be the location based service resources, discount coupons or monetary awards. It is assumed that the more accurate the information, the more valuable it is for the company. For example, street level information leads to contextual advertisements while city level granularity is less valuable. Concurrently, by being less anonymous, the users take a privacy risk. We take a commodity view of the privacy here, where the users can trade their privacy to obtain benefits from the company in an individual risk aware way. The model of the privacy mechanism is given next.

4.2 Privacy Mechanism Model

Consider a mobile network composed of a set of mobile users with cardinality N. Around user i at any time t, let a group of $n_i(t)$ mobile users, $\mathscr{A}$, are in close proximity in an area. The service provider gives location based applications to the mobile users. Therefore, it asks for the location information from the mobiles.

Table 4.1: Values of $n_i(t)$, N and g

$n_i(t)$	N	g
10^1	10^3	$\frac{2}{3}$
10^3	10^6	$\frac{1}{2}$
10^6	10^9	$\frac{1}{3}$

We use an information theoretic approach to quantify the anonymity level of the individual mobile users while giving the location information. The uncertainty of service provider about the location information of user i is defined using the entropy term

$$A_i = \sum_{j=1}^{n_i(t)} p_j \log_2 \frac{1}{p_j}, \tag{4.1}$$

where probability p_j corresponds to the probability that a user j is in a location. The parameter A_i concurrently quantifies the anonymity level of a users i. We can see that $p_i = \frac{1}{\log_2 n_i(t)}$. Then A_i simply boils down to,

$$A_i = \log_2 n_i(t).$$

We next define a metric called *granularity of location information*, g_i, for the i^{th} user as

$$g_i = 1 - \frac{A_i}{\log_2 N}.$$

The value of g_i is between zero and one for each user. The anonymity level obtained by user i by reporting with a granularity level g_i is

$$A_i = (1 - g_i)\ \log_2 N.$$

Here, $g_i = 0$ means the user i keeps its location completely private and $g_i = 1$ means the user gives exact location to the mobile company. We can see that the more the value of $\mathbf{g}$, the less anonymous are the users. With a given value of g_i the users specify the size of the crowd it belongs to, i.e., $n_i(t)$. The Table 4.1 gives values of g for different combinations of $n_i(t)$ and N. We can see that as the size of the population N increases the more anonymous become the users.

The users decide on the value of g which they report to the company. In the scenario considered in this model, the users have a continuous decision space resulting from a risk-benefit trade-off optimization, i.e. the allowed decisions are not just full or null information. This allows the designer to provide benefit based on the level of information given by the users.

There is a cost of perceived risk c_i associated with the user's privacy when they give location information, which linearly increases with the granularity of information, i.e,

$$c_i = r_i g_i, \ \forall i,$$

where r_i is the risk factor. The risk factor may result from disclosing your daily routine or behavior to unknown parties. For example, the users may not like others to know when they are in their office or home or they may simply care about their privacy on principle. The users estimate or learn about their risk level from past experiences or from reliable sources or by exchanging information with users like how much level of g with which they report to the designer.

While gaining on location privacy, each user loses on the benefits of location based applications/services due to the anonymity. For example, while depending on whether users are in office, home or a particular street or city, they might be targeted with different kinds of offers and services. When they give wrong information they are given wrong services and offers. The total benefit obtained by user i can be quantified as

$$s_i = b_i(\mathbf{g}) \log(1 + g_i),$$

where $b_i(\mathbf{g}) \in R^+$ is the benefit or subsidy factor provided by the company. Note that the benefit factor b_i provided for user i is designed based on the granularity level chosen by all the users. In other words, the company provides benefits based on the total available information in the actual "information market". We model that the total benefit increases logarithmically with the granularity level, since for low granularity level marginal increase in the value of location information is higher. The logarithmic assumption in this chapter can be generalized to any nondecreasing, concave function.

We now summarize the definitions of some of the terms discussed so far.

Definition 4.1 (Location Privacy)**.** Location privacy of an individual user refers to how she discloses and controls the dissemination of her personal (location) data.

Definition 4.2 (Anonymity (location))**.** Anonymity of a user i, A_i, is the uncertainty of the service provider about the users location.

$$A_i = \sum_{i=1}^{n_i(t)} p_i \log_2 \frac{1}{p_i}.$$

Definition 4.3 (Granularity of Information)**.** Granularity of information is the level of granularity with which a user i reports its location.

$$g_i = 1 - \frac{A_i}{\log_2 N}.$$

Definition 4.4 (Perceived risk (cost))**.** It is the total cost perceived by user i as a result of reporting her location with a certain level of granularity of information, which is modeled as linear in g_i,

$$c_i = r_i g_i.$$

Definition 4.5 (Benefit)**.** The total subsidy or reward user i obtains from the mobile commerce company by disclosing her location with a certain level of granularity of information,

$$s_i = b_i(\mathbf{g}) \log(1 + g_i).$$

In a mechanism design setting, there is a *designer* D at the center who influences N *players* participating in a **strategic (non cooperative) game**. Let us define the interaction of the users in the close proximity in the above setting as an N-player strategic game, $\mathscr{G}$, where each player $i \in A$ has a respective **decision variable** g_i such that

$$g = [g_1, \ldots, g_N] \in \mathscr{X} \subset \Re^N,$$

where X is the decision space of all players. The cost of each mobile user i will be the risk it perceives minus the benefits it obtains from the company, i.e.,

$$J_i(g) = r_i g_i - b_i \log(1 + g_i) \; \forall i.$$

Each mobile user then solves her own optimization problem

$$\min_{g_i} J_i(\mathbf{g}). \tag{4.2}$$

Note that from the price taking user perspective, the benefit b_i is a constant designed by the company, since each user has an information constraint to know the granularity level of other users and calculate its benefit. The users just take best response given the benefit provided by the company.

The company acts here as the mechanism designer and has the goal of obtaining a desired level of location information granularity from the users. In this chapter, the designer has an unconventional objective compared to other works in mechanism design where the designer usually looks for social welfare or designer revenue maximization. The designer or company here wants to improve the precision of location information from each user, which is captured by a designer objective function that takes granularity of information of all the users as its argument. The designer objective we consider here is,

$$\max_{\mathbf{b}} V = \max_{\mathbf{b}} \sum_{i=1}^{N} w_i \log(1 + g_i(b_i)), \tag{4.3}$$

subject to a budget or resource constraint

$$\sum_{i=1}^{N} b_i \leq B$$

where w_i's are the weights given to individual users as desired by the designer and B is the total budget. The weights depend on how much the company values the location information from different types of users.

It is important to note here that the designer (the mobile commerce company) tries to achieves its objective indirectly by providing benefits to users $\mathbf{b}$ as it naturally does not have control on their behavior, i.e. $\mathbf{g}$. Essentially, the company tries to move the NE point vector of $\mathbf{g}$ of the resulting game to a desirable point by using the benefits provided to the users.

4.3 Location Privacy Mechanism

In a privacy mechanism, each user decides on the location privacy level to be reported, i.e., g_i, depending on its risk level perception as a best response to the benefit set by the company by minimizing individual cost. The underlying game may converge to a Nash equilibrium, which may not be desirable to the service provider because the required level of location information not obtained. Therefore, the designer employs a pricing or subsidy mechanism to motivate the users by properly selecting the benefits delivered to each user by solving a global objective. We obtain the optimum benefit for each user by aligning user problems and designer problem as,

$$b_i^* = \frac{w_i}{\nu^* + \lambda_i^* - \mu_i^*}, \ \forall i \in \mathscr{A}, \tag{4.4}$$

where $\nu^*, \lambda_i^*, \mu_i^*$ are Lagrange multipliers. Then, the optimal granularity level of each user will be,

$$g_i = \begin{cases} 0, & \text{if } b_i \leq r_i \\ \dfrac{w_i}{(\nu^* + \lambda_i^* - \mu_i^*) r_i} - 1, & \text{if } r_i \leq b_i \leq 2r_i \\ 1, & \text{if } b_i \geq 2r_i. \end{cases}$$

The designer can obtain desired granularity of information from each user by properly

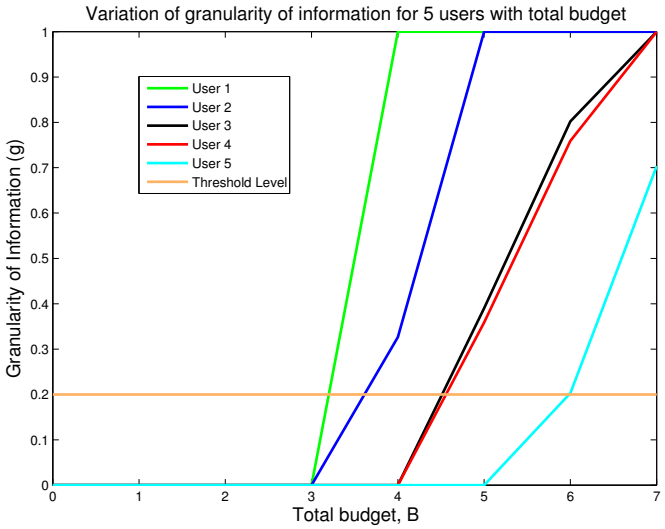

Figure 4.1: Granularity of information of 5 users with the total budget.

selecting the functions in the global objective and the weights in the function. Note that to formulate the objective and for imposing the constraints on the global problem, the designer needs to know the user r's.

4.4 Numerical Analysis

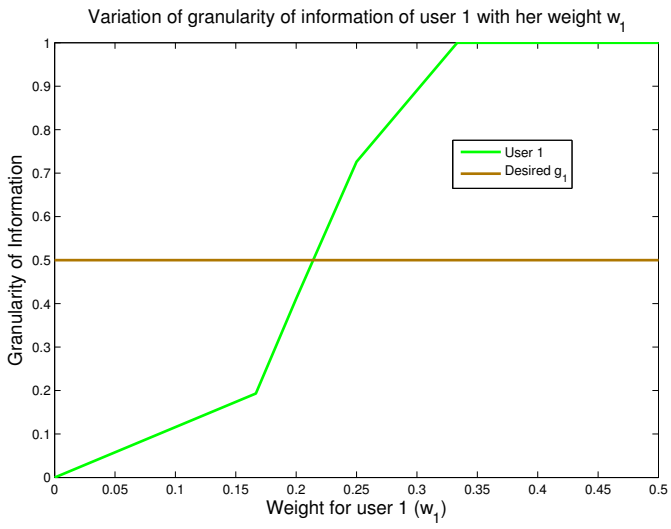

Figure 4.2: Variation of granularity of information of user 1 with the weight in the global objective.

The privacy mechanism given in Section 4.3 is illustrated with a numerical example in this section. We considered 5 users having logarithmic utilities and their risk factors are randomly generated between 0 and 2. The risk vector in an instance is taken as

$$r = [0.18\, 0.45\, 0.89\, 0.98\, 1.1693].$$

The weights given to the users in the global objective is taken as

$$w = [1.78\, 0.945\, 0.99\, 1.098\, 0.869]$$

and assumed that the company has no control over these weights to manipulate them. We first plotted the variation of the best response granularity level of the users with the total budget of the company in Figure 4.1.

We can observe in Figure 4.1 that there is a critical budget below which the company cannot extract any location information from the users. We could also observe from Figure 4.1 that the company can extract more and more granularity of information by increasing the total budget, as expected. The threshold level of granularity for all the users which is the minimum level required to provide the service is taken to be 0.2. The level of budget required for extracting more than this threshold level of granularity from all the users, can be obtained from Figure 4.1. For the instance considered in the plot, the critical level of budget is given as 6. Next, we consider the case where the company can adjust the weight given to different users in the global objective. In Figure 4.2, the setting remains as in the Figure 4.1 except that the company varies the weight of the

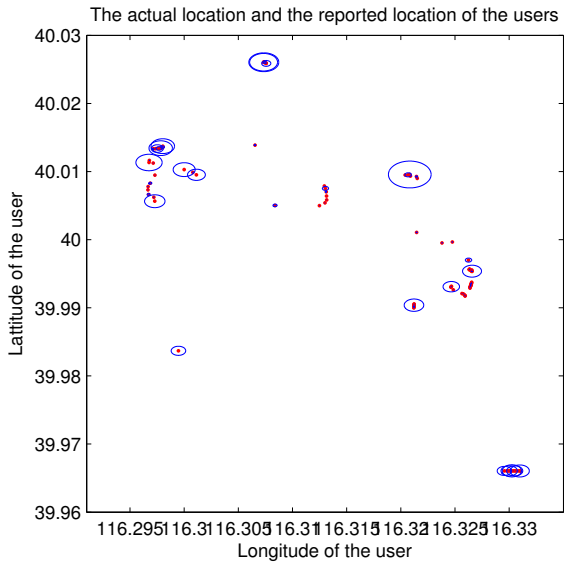

Figure 4.3: Location of users: Actual and Reported.

first user. From this plot, the weight required to get the desired level of granularity of information can be obtained. For user 1 the desired level of granularity of information is obtained with $w_1 = 0.21$.

4.4.1 Simulation Results

We construct the location of large number of users and the crowd around them from their reported granularity level using real dataset here. We use the GPS trajectory dataset ([123, 121, 122]) which was collected in (Microsoft Research Asia) Geolife project by 167 users in a period of over three years from April 2007 to December 2010. These data sets give context information to the systems and help to develop innovative mobile and web application. They also help to infer the user transportation modes and mobility patterns. But the users need to be incentivised to share their location for obtaining these data sets. The data set which gives the latitude and longitude of 160 users at different times from 2007 to 2010 is imported for a particular time. Using these latitude and longitude information, the exact location of the users are plotted in the Figure 4.3. We obtained the best response granularity level of the users from the privacy mechanism in Section 4.3 for the case of logarithmic utility function for a particular risk vector and budget. These best response granularity levels are mapped back to the size of the crowd ($n_i(t)$) from the equation (4.1) given in Section 4.2 and reported locations are constructed from them.

The location anonymity of the users due to the granularity level they reported in equilibrium are represented as the circles around the actual locations using the data set

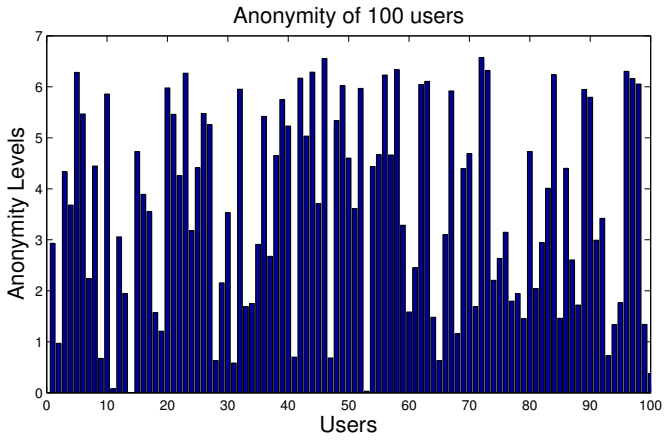

Figure 4.4: Anonymity levels of users.

in the Figure 4.3. The blue circle around a user contains the crowd of users around that particular user. We can observe that users have different size of crowd around them depending on the risk factor they have. From the plot we can understand that if we consider the users does not share their actual location but act according to the privacy mechanism, we get a map of users with the blue circles instead of the read dots. The company will have to modify the location based application taking this into consideration.

Next we plot the anonymity levels chosen by the users in the equilibrium. Depending on the values of n_i each user i will have a number of users around her and the anonymity levels according to that. The anonymity levels of the 100 users are plotted as a bar graph in the Figure 4.4.

4.5 Conclusion

I this chapter we modeled and analyzed the interaction of a mobile commerce company with its users who obtain location based services, as a strategic game. A privacy mechanism has been designed where the company motivates its users to report their location information at a granularity level desired by the company. In return, monetary benefits are obtained by a user depending on the granularity level taken by them and on the weight the designer gives for them in the global objective. It has been observed that, the users report their location with nonzero granularity level of information when the subsidy by the company exceeds their perceived risk factor.

5 Iterative Algorithms and Learning for Mechanisms

5.1 Introduction

We consider the implementation of pricing mechanisms which were proposed in the earlier chapters in this chapter. We considered one shot games in the previous chapters and now we consider that the users interact over a time to converge to the NE point. We first consider the iterative and distributed algorithms in which the users and the designer update their strategies and prices in a gradient manner. We prove the convergence of the algorithm in Section 3.2.2 of Chapter 3.

Next, the mechanism designer learns these utility functions using regression techniques based on the bids reported or actions taken by the users. Specifically, a *Gaussian process regression learning* [92] technique is used to estimate the marginal utilities of the players. The best response of the players to the prices and rules imposed by the designer constitutes the training data set. Once the marginal utilities are estimated with small number of training data points, the optimal point is searched in order to satisfy the optimality conditions. The nature of the optimal point may depend on the specific problem formulation. In the specific problem considered here, the optimality condition becomes full utilization of the resource given the marginal utilities of the users.

In pricing mechanisms, the price taking players take best response actions to the the price charged by the designer. We use Gaussian process regression learning to approximate the utility function of players from the 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.

5.2 Convergence Analysis of Iterative Algorithms

Here we analyze the convergence of the iterative distributed algorithm for the pricing mechanism given in Section 3.2.2 of Chapter 3. . First, we consider an iterative algorithm to iteratively compute the NE solution of the mechanism, with single carrier. Let the

iterative distributed mechanism be $\mathscr{M}_c'$ is defined by the following equations,

$$x_i(k+1) = x_i(k) - \kappa_i \frac{\partial J_i}{\partial x_i} \quad \forall i \in \mathbf{A}, \tag{5.1}$$

$$\lambda(k+1) = [\lambda(k) - \kappa_D\big(\sum_i x_i(k+1) - X_{max}\big)]^+, \tag{5.2}$$

where $[s]^+ = \max(0, s)$.

Theorem 5.1. *In the iterative pricing mechanism $\mathscr{M}_c'$ defined by the set of equations (5.1) and (5.2) converges to a unique point in the constraint set individually if $0 < \kappa_i < \frac{2}{M_1}, \forall i$ and $0 < \kappa_D < \frac{2}{M_2}$, where M_1 is the constant which bounds $||\Gamma(\delta J_i(\mathbf{x}))||, \forall \mathbf{x} \in \mathscr{A}$ and M_2 is the constant which bounds $||\Gamma(\delta L(\lambda))||, \forall \lambda \in \Re_n^+$ and Γ is the Jacobian matrix. The algorithm converges to a unique point assuming that the Lagrange multiplier update in (5.2) happens in a slower time scale than the user action updates in (5.1).*

Proof. In [17], for analyzing constraint optimization problems, the infeasible points are projected back to the feasible region. The projection mapping is defined as,

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

where $\mathbf{X}$ is the feasible set.

For the convergence of the gradient projection algorithm, the relaxations of Assumptions 3.1 given in [17] (pp. 213) are to be satisfied as sufficient conditions. The relaxed Assumption 3.1 says that $F(\mathbf{x}) > c, \forall \mathbf{x} \in X$ for a $c \in \Re$ for any F to be minimized. Both user cost function and the global objective satisfy this. The second assumption is the Lipschitz continuity condition given by,

$$||\delta J_i(\mathbf{x}) - \delta J_i(\mathbf{y})|| \leq K||\mathbf{x} - \mathbf{y}||, \forall \mathbf{x}, \mathbf{y} \in \mathscr{X}.$$

The user cost functions are twice continuously differentiable from the Assumption 2.4. Therefore, we can use the mean value theorem for vector valued functions which states that,

$$\delta J_i(\mathbf{x}) - \delta J_i(\mathbf{y}) = (\int_0^1 \Gamma(\delta J_i(\mathbf{y} + t\rho)dt)) \cdot (\mathbf{x} - \mathbf{y}), \forall \mathbf{x}, \mathbf{y} \in \mathbf{X}, \forall i$$

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

$$\Gamma(\delta J_i(\mathbf{x})) := \begin{pmatrix} c_1 & c_{12} & \cdots & c_{1N} \\ c_{21} & c_2 & \cdots & c_{2N} \\ \vdots & & \ddots & \vdots \\ c_{N1} & c_{N2} & \cdots & c_N \end{pmatrix}, \tag{5.3}$$

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

Using the Cauchy-Schwartz inequality,

$$||\delta J_i(\mathbf{x}) - \delta J_i(\mathbf{y})|| \leq M_1||\mathbf{x} - \mathbf{y}||, \forall \mathbf{x}, \mathbf{y} \in \mathscr{X}, \forall i, \tag{5.4}$$

where M_1 is the constant which bounds $||\Gamma(\delta J_i(\mathbf{x}))||, \forall \mathbf{x} \in \mathscr{X}$. The set $\mathscr{X}$ is convex here and $(y + t\rho) \in S$ for t between 0 and 1. For $x \in X$, M_1 is bounded when the boundaries of S are finite. Therefore, the action update according to equations (5.1) converges if $0 < \kappa_i < \frac{2}{M_1}, \forall i \in A$ 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 (5.1),

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

Therefore, the gradient update using user cost in (5.1) is according to the gradient update of the global objective.

The Lagrange function of the global objective is given by

$$L(\mathbf{x}) = \sum_i U_i(\mathbf{x}) - \lambda(\sum_i x_i - X_{max}).$$

subject to the condition that $\lambda \geq 0, \forall i$. The gradient descent equation for $L(\mathbf{x})$ is given by

$$\lambda(k+1) = [\lambda(k) + \kappa_D \frac{\partial L}{\partial \lambda}]^+ \ \forall i. \tag{5.5}$$

It can be verified easily that the equation (5.2) is equivalent to equation (5.5).

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

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

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 (5.2) converges if $0 < \kappa_D < \frac{2}{M_2}$, for given action vector x. Gradient descent equations under the above assumptions converges according to Prop. 3.4. in [17] (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 [17]. 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. □

Remark 5.1. The proof can be easily generalized to the multi-carrier systems and energy minimization objective.

5.3 Regression Learning of Utility Functions

The users have utility functions private to them which are functions on their actions x. Therefore, the designer can learn these utility functions from the actions taken by the users. Consider any function $f(.)$ and a set of M data points $\mathbf{E} = \{x_1, \ldots, x_M\}$, and the corresponding vector of scalar values is $\{f(x_1), f(x_2)...., f(x_M)\}$. A regression learning algorithm uses the training data set to give a learned function $\hat{f}$ which minimizes the error from f and follows the real shape of f. Assume that the observations are distorted by a zero-mean Gaussian noise, n with variance $\sigma \sim N(0, \sigma)$. Then, the resulting observations is a vector of Gaussian $y = f(x) + n \sim N(f(x), \sigma)$.

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

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

and

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

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* $W(x, \tilde{x})$ and the diagonal noise variance

$$C(x, \tilde{x}) = W(x, \tilde{x}) + \sigma I,\ \forall\, x, \tilde{x} \in \mathscr{E}, \tag{5.6}$$

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

$$W(x, \tilde{x}) = \exp\left[-\frac{1}{2}\left\|x - \tilde{x}\right\|^2\right]. \tag{5.7}$$

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

$$k(\bar{x}) = [W(x_1, \bar{x}), \ldots W(x_M, \bar{x})] \tag{5.8}$$

and scalar

$$\kappa = W(\bar{x}, \bar{x}) + \sigma. \tag{5.9}$$

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

$$\hat{f}(\bar{x}) = k^T C^{-1} y \text{ and } v(\bar{x}) = \kappa - k^T C^{-1} k. \tag{5.10}$$

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 $\hat{f}$.

Here the designer learns the marginal utility functions U_i' of each user using their best response bids or actions as data points.

5.3.1 Learning in Pricing Mechanisms

In this section, regression techniques are used to learn the user private marginal utilities by the designer for implementation of pricing mechanisms.

We consider the case of a divisible resource of amount X_{max} is allocated among users having separable utility functions. The resource can be spectrum in wireless communication systems or bandwidth in the Internet. Due to the selfish nature of the individual users, without designer intervention there will be an inefficient distribution of the divisible resource (Price of Anarchy). The prices are designed to bring the Nash Equilibrium of the resulting game to an efficient point.

The user optimization problem will be to find the action level which minimizes his individual cost , i.e.,

$$\min_{x_i} \quad P_i x_i - U_i(x_i).$$

Consequently, the general condition for player best response obtained from first order derivative is

$$P_i - \frac{dU_i(x_i)}{dx_i} = 0, \ \forall \ i \in A. \tag{5.11}$$

The best response will be,

$$x_i = (\frac{dU_i}{dx_i})^{-1}(P_i), \ \forall \ i \in A. \tag{5.12}$$

The designer want to achieve the maximum social welfare, i.e the net utility of users is to be maximized. Therefore, the social objective is,

$$V = \max_x \sum_i U_i(x_i), \text{such that} \sum_i x_i \leq X_{max}.$$

The Lagrangian is given by

$$L = \sum_i U_i(x_i) + \lambda(\sum_i x_i - X_{max}).$$

where $\lambda > 0$ is the unique Lagrange multiplier.

The resulting Karush-Kuhn-Tucker (KKT) conditions will give,

$$U_i'(x_i) = \lambda, \ \forall i \in A, \tag{5.13}$$

and

$$\lambda(\sum_i x_i - X_{max}) = 0, \ \forall i,$$

Since the individual user utility functions are concave and non-decreasing, the optimum point will ensure boundary solution. By comparing (5.13) and (5.11), we conclude that for aligning designer and user objectives, the designer needs to set λ as the price for every user for solving designer and user problems. Therefore, from the criterion of full resource usage, it follows that

$$\sum_i x_i^* = \sum_i \left(U_i'\right)^{-1}(\lambda^*) = X_{max}. \tag{5.14}$$

where x^* and λ^* are the optimal points.

Each user i sends a response to the sample prices $\{P_{i1}, \cdots, P_{iM}\}$ set by the social planner which contains the action vector $\{x_{i1}, \cdots, x_{iM}\}$. The corresponding scalar marginal utility values at those points are $U_i'(x_{i1}, \cdots, U_i'(x_{iM}) \ , \forall i$. Assume that the observations are distorted by a zero-mean Gaussian noise, n with variance $\sigma \sim N(0, \sigma)$. Now let the Gaussian vector obtained in the case of user i is $\{y_{i1}, \cdots, y_{iM}\}$, where

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

A Gaussian regression technique as described is used to estimate the marginal utility functions $\tilde{U_i'}$. After that, the λ values are obtained by an online learning algorithm. The optimal points λ^* and x^* are selected at which

$$\lambda^* = \tilde{U_i'} = \tilde{U_j'}, \forall i, j$$

and $\sum_i x_i^* = X_{max}$.

The algorithm which also shows the information flow for the regression learning method is given below in Algorithm 2. First an initial estimation of marginal utilities are obtained using M data points. Then the best value of λ is found using an iterative search by the designer

$$\lambda_{n+1} = \lambda_n + \kappa_D\big(\sum_i x_i - X_{max}\big), \tag{5.15}$$

where n is the time step and κ_D is the step size. The corresponding values of x are obtained using the estimated marginal utility curves by setting λ_n as the marginal utility values. By checking the full utilization condition the converging value λ_{new} is obtained. It is important to note that this computation is done by the designer alone and does not require any player involvement. The converged value λ_{new} is sent to the players as the new prices, and new actions x_{new} are observed. The noisy version of value of λ_{new} (which is the value of the function at x_{new}) and x_{new} are added next to the initial data set. Using the regression this new data set gives a better estimate of marginal utilities near the optimal point. From this new estimate of marginal utilities the iteration given by equation (5.15) is run to obtain a new converging value of λ and corresponding values of x. This online learning and estimation is repeated till end of iteration.

Remark 5.2. Note that by using the online learning algorithm as above, when the user preferences or parameters in utility function change in the course of time, the designer

Algorithm 2: Regression Learning of User Utilities in Pricing Mechanisms

Input: *Designer*: Global objective.
Input: *Players (users)*: Utility functions $U_i(x_i)$
Result: Learned utility functions $\tilde{U}_i(x)\ \forall i$, optimal prices, and efficient allocation vector x^*

Initialization: The designer obtains initial data points by selecting values for the Lagrangian λ and makes an initial estimate of $\tilde{U}_i$ for each user i using GP by setting the prices accordingly and observing user responses;
repeat
  begin *Designer:*
    Update the value of λ using $\lambda_{n+1} = \lambda_n + \kappa_D\big(\sum_i x_i - X_{max}\big)$;
    Using $\tilde{U}_i$, find the corresponding values of x;
    Continue until $\sum_i x_i = X_{max}$ **and denote the corresponding** λ_n **as** λ_{new};
    Set λ_{new} **as the user prices,** P_i ;
    begin *Players:*
      foreach *Player* i **do**
        Take action x_{inew} as response to the prices P_i;
      end
    end
    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*;

can estimate the new functions and can move the system to optimal point. The numerical results which illustrate the learned functions and convergence of the algorithm are given in Section 5.4. We observe that by using this online learning algorithm, the designer can adapt the estimation if the utility functions or utility parameters of the players change in the course of time.

5.3.2 Learning in Auctions

We consider next iterative auctions similar to iterative combinatorial auction or English auction for a divisible good. The players decide on their bids or actions by minimizing their cost which is a combination of their own utilities and prices imposed by the designer. Specifically, the designer D imposes on a player $i \in A$ a user-specific resource allocation rule, $Q_i(x)$, pricing, $P_i(x)$ from the the vector of player bids x. We consider here an additive resource sharing scenario where the players bid for a fixed divisible resource Q_{max} and are allocated their share captured by the vector $Q = [Q_1, \ldots, Q_N]$ subject to the resource constraint $\sum_i Q_i \leq Q_{max}$.

The total payment by the i^{th} player is $c_i(x) = P_i(x)Q_i(x)$. The player utility function U_i is separable, i.e. it depends only on the individual allocation of the player. It is also assumed to be continuous, strictly concave, and twice differentiable in terms of its argument Q_i.

From a player's perspective, who takes myopic best response to the price and allocation given by the designer and tries to minimize its cost in terms of the actual resources obtained, the condition

$$\frac{\partial J_i}{\partial Q_i} = \frac{\partial c_i}{\partial Q_i} - \frac{\partial U_i}{\partial Q_i} = c_i' - U_i'$$

is necessary and sufficient for optimality. Suppressing the dependence of user cost on bids x, for the cost minimization, it has to satisfy

$$P_i(Q) = \frac{\partial U_i(Q_i)}{\partial Q_i} \quad \forall i \in A. \tag{5.16}$$

Furthermore, if additional assumptions are made on $J_i(x)$, it can be shown that the game admits a unique NE, Q^* (or x^*) [13].

Different from players, the designer D has two objectives: maximizing the sum of utilities of players and allocating all of the existing resource Q_{max}, i.e. its full utilization. Hence, the designer D solves the constrained optimization problem

$$\max_Q V(Q) \Leftrightarrow \max_Q \sum_i U_i(Q_i) \text{ such that } \sum_i Q_i \leq Q_{max}, \tag{5.17}$$

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

$$L(Q) = \sum_i U_i(Q_i) + \lambda \left(Q_{max} - \sum_i Q_i \right),$$

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

$$\frac{\partial L}{\partial Q_i} \Rightarrow U_i'(Q_i) = \lambda, \ \forall i \in A, \tag{5.18}$$

and the efficiency constraint

$$\frac{\partial L}{\partial \lambda} \Rightarrow \sum_i Q_i = Q_{max}. \tag{5.19}$$

In the specific resource sharing setting defined, an auction-based mechanism, $\mathscr{M}_a$, can be defined based on the bid of player i,

$$x_i := P_i(x)Q_i(x), \tag{5.20}$$

the pricing function

$$P_i := \frac{\sum_{j \neq i} x_j + \omega}{Q_{max}}, \tag{5.21}$$

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

$$Q_i := \frac{x_i}{\sum_{j \neq i} x_j + \omega} Q_{max}. \tag{5.22}$$

which is differentiable. It is also possible to interpret the scalar ω as a *reserve bid* [57]. Note that the bid of each player is her willingness to pay i.e. the total amount she pays is her bid $c_i(x) = x_i$. The cost function for the mechanism $\mathscr{M}_a$ becomes in this case,

$$J_i(x) = x_i - U_i(Q_i(x)). \tag{5.23}$$

Let us denote

$$S_i = \sum_{j \neq i} x_j + \omega,$$

and then equations (5.21) and (5.22) become

$$P_i := \frac{S_i}{Q_{max}}, \tag{5.24}$$

and

$$Q_i := \frac{x_i}{S_i} Q_{max}. \tag{5.25}$$

We obtain the best response as,

$$Q_i^* = \left(\frac{\partial U_i}{\partial Q_i}\right)^{-1} (\frac{S_i}{Q_{max}}), \tag{5.26}$$

where S_i/Q_{max} is the argument of the inverse marginal utility function.

From the general condition in equation (5.16), the marginal utility is equal to the price

$$\frac{\partial U_i}{\partial Q_i} = \frac{S_i}{Q_{max}} = \frac{\sum_{j \neq i} x_j + \omega}{Q_{max}}. \tag{5.27}$$

This equation can be rewritten as following

$$\frac{\partial U_i}{\partial Q_i}(x_i) = \psi(x) - \frac{x_i}{Q_{max}}. \tag{5.28}$$

where

$$\psi(x) = \frac{\sum_j x_j + \omega}{Q_{max}}. \tag{5.29}$$

As in pricing, GP regression learning is used now to learn the marginal utilities in auctions. For an initial value of ω, an initial estimate of the marginal utilities of players are constructed. The values of Q_i's will give the corresponding values of x_i's for this initial value of ω.

Next, the value of ψ is varied over space of all possible values, by changing the value of the reserve bid ω. This search algorithm provides the value of λ for which $\sum_i Q_i = Q_{max}$ for any general utility function and the corresponding value of ω. This ω is then used to set the price and allocation, using which the bids will converge to the efficient point. Since the reserve bid is an independent parameter which does not depend on user bids, the incentive compatible property of the mechanism still holds.

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

$$U_i = \alpha_i \log Q_i \;\; \forall i \in A.$$

The best response is $x_i^* = \alpha_i$. The unknown α's are then learned in single step from the bid which corresponds to optimal point.

Consider next the alternative case of exponential user utilities,

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

In this case

$$x_i^* = \frac{S_i}{Q_{max}\alpha_i} \log \frac{Q_{max}}{S_i}.$$

So to learn α's an iteration is needed and the optimal prices based on these correct α's will take the system to approximately efficient point.

In the case of general user utilities, however, multiple steps of the Algorithm 2 are required in order for the designer to characterize user utilities with sufficient accuracy and the outcome converges to the optimal solution.

5.4 Numerical Results

In this section we provide some numerical results that illustrate our theoretical analysis. We consider a system with 5 users having scalar parametrized logarithmic utility functions in order to visualize the results.

In Figure 5.1, 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 Algorithm 2. 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.

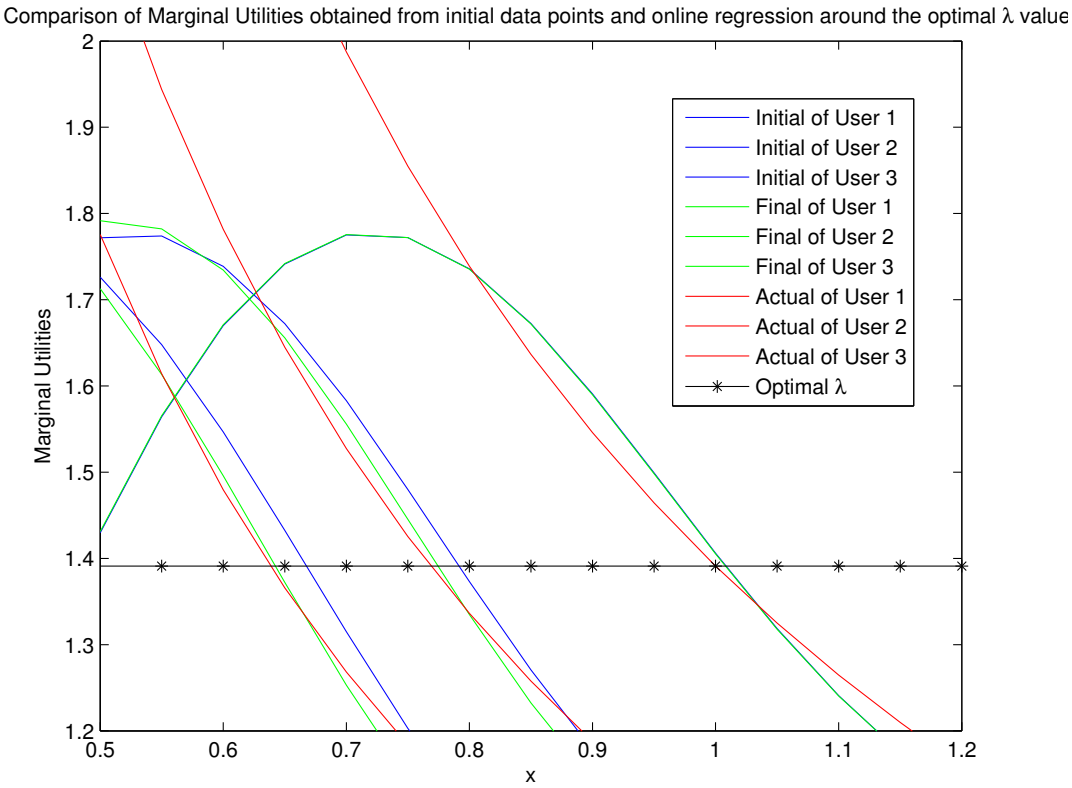

Figure 5.1: Marginal Utility curve for logarithmic utilities constructed using initial data points and the online algorithm given in Algorithm 2.

5.5 Conclusion

The convergence of the iterative algorithm, which was proposed in Cahpter 3, has been proven for a single carrier case. The rest of the chapter has analyzed a scenario in which the mechanism designer uses learning techniques as a tool for estimating the utilities of the players. We have considered the problem of allocation of a divisible resource by a designer to a number of players having infinite dimensional utility functions and designer employing Gaussian process regression method to obtain the marginal utility functions of the players. In the pricing mechanisms, the Lagrange multiplier of the total resource constraint, which is set as the price for all the users, has been used to navigate the allocation to the efficient point using the estimated marginal utilities. In auctions, the reserve bid parameter in the pricing and allocation rule has been varied for obtaining near efficient point. We have also proposed an online algorithm which uses the best response action of users in each time instance to give a better estimate of the utilities, near the efficient point.

6 Mechanism Design with Malicious Users

6.1 Introduction

In this chapter, we model the coexistence of altruistic, selfish and malicious players by introducing an overarching noncooperative game-theoretic framework. Specifically, we adopt a mechanism design ([72], [4]) approach in which a set of rules and incentives are used to control the outcome of the underlying game between the players. Within the framework developed, we study the effect of malicious players on mechanisms where the regular players exhibit selfish behavior. Here, we assume that malicious users mainly stay within the rules of the system. Hence, the are modeled by assigning different utility functions than the selfish players, for example a common 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 [112] is an efficient and strategy-proof (truth revealing) mechanism in the presence of selfish players. We first show the effect of the adversarial behavior of some users on the efficiency of VCG mechanism for allocation of divisible resources, which is used to motivate the need for quantifying the effect of adversarial behavior on network mechanisms.

To quantify the effects of adversarial behavior, we analyze the robustness of some known network mechanisms with respect to the adversarial behavior of (some of) their participants. The metric called Price of Malice [84]-[12] is modified for network resource allocation games and applied to two different network problems studied 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 arises when some of the malicious users form a group or *collusion* in order to disrupt mechanisms. The mechanisms that are resistant to collusion are called group strategy-proof mechanisms. In Section 6.4.1, we investigate the group strategy-proof property of one of the mechanisms proposed for network resource sharing setting and in Section 6.4.2 quantify the effect of adversarial behavior resulting from collusion.

To counter the adversarial behavior, we design mechanisms in which the prices are varied differentially to punish the malicious players after detecting them using a threshold detection technique based on the bids of users. Clearly, when the malicious users do not abide by the rules and vandalize the system, a stronger response such as blocking the users suspected of malicious behavior after detection is 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.

We consider two different types of network problems in this thesis which differ in coupling of users 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, which is often referred as Price of Anarchy. Mechanisms such as auctions and pricing schemes have been proposed to shift the Nash equilibrium point to efficient point. In these mechanisms and underlying games, the selfish nature of rational users have been modeled with concave utility functions. In practical situations, however, there are altruistic users who care for the welfare of all the users as well as adversarial users who may deviate from equilibrium point even if it causes a 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 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*.

This chapter studies the effects of and countermeasures against adversarial behavior in network resource allocation mechanisms such as auctions and pricing schemes. It models the heterogeneous behavior of users, which ranges from altruistic to selfish and to malicious, within the analytical framework of game theory. A mechanism design approach is adopted to quantify the effect of adversarial behavior, which ranges from extreme selfishness to destructive maliciousness. First, the well-known result on the Vicrey-Clarke-Groves (VCG) mechanism losing its efficiency property in the presence of malicious users is extended to the case of divisible resource allocation to motivate the need to quantify the effect of malicious behavior. Then, the *Price of Malice* of the VCG mechanism and of some other network mechanisms are derived. The resistance of a mechanism to collusion is investigated next and the effect of collusion of some malicious users is quantified. Differentiated pricing as a method to counter adversarial behaviors is proposed and briefly discussed. The results obtained are illustrated with numerical examples and simulations in Section 6.6.

We focus on two basic types of resource sharing and coupling in this chapter, which are often encountered in a variety of networking problems:

1. *Additive resource sharing:* The players share a finite resource Q_{max} such that

$$\sum_{i=1}^{N} Q_i = Q_{max}.$$

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

2. *Interference coupling* (linear interference): The resource allocated to player i, γ_i, is inversely proportional to interference generated by others. Interference coupling

occurs in wireless networks where γ represents signal-to-interference-plus-noise ratio(SINR). For example, in a single carrier CDMA system, SINR is given by

$$\gamma_i(\mathbf{Q}) = \frac{Q_i}{\frac{1}{L}\sum_{j\neq i} Q_j + \sigma^2}, \tag{6.1}$$

from equation (3.1). The individual power of the users will be $\frac{Q_i}{h_i}$ where $h_i\ \forall i$ are the channel gains.

6.1.1 Adversarial behavior in VCG Mechanism

First, we show the effect of malicious behavior in VCG mechanism, which is a direct mechanism where the users submit their entire utility function to the designer. For this case the strategy space $\mathscr{X}$ is infinite dimensional. We consider logarithmic utility functions,

$$U_i(\mathbf{x}) = \alpha_i \log(Q_i(x)), \forall i. \tag{6.2}$$

For the case where user utility functions are parametrized by a scalar value α, each user reports its α and θ, i.e.,$\mathscr{X} \subset \Re^{2N}$. Unlike in the classical VCG mechanism, where all the users are selfish, we consider some users as malicious who reports a malicious utility function $U_i^m(\mathbf{x})$ to the designer, instead of a regular selfish utility $U_i(\mathbf{x})$. We show in this section, the effect of malicious behavior in VCG mechanism for allocation of divisible resources and here we do not follow a Bayesian approach as in [87].

When allocating a single divisible resource of quantity Q_{max}, the efficient allocation and total VCG payment for a user i, in the presence of other heterogeneous users, is

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

and

$$C_i^{VCG} = -\sum_{j\neq i} U_j^m(Q_j^*(x)) + \sum_{j\neq i} U_j^m(Q_j^i(x)), \forall i, \tag{6.3}$$

where

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

is the efficient allocation when user i is out of the system. The optimizations above are subject to the constraint $\sum_i Q_i = Q_{max}$.

As result of this allocation and payment the individual cost of the users become

$$J_i = C_i^{VCG} - U_i^m(Q_i^*(\mathbf{x})), \forall i.$$

In the case of logarithmic user utility functions parameterized by a scalar value, when none of the user is malicious, the allocation and payment become

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

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

Consider the case where only user k is malicious and reports U_k^m to the designer to reduce the share of resource allocation to the other selfish users. Then, the optimal allocation becomes

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

Again, in the case of logarithmic user utility functions, we have

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

The individual user allocations are given in the malicious case as

$$Q_k^{m*} = \frac{\alpha_k X_{max}}{\alpha_k + (1+\theta_k) \sum_{j \neq k} \alpha_j}, \tag{6.4}$$

$$Q_j^{m*} = \frac{\alpha_j (1+\theta_k) X_{max}}{\alpha_k + (1+\theta_k) \sum_{j \neq k} \alpha_j}, \forall j \neq k. \tag{6.5}$$

We observe 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. Therefore, we conclude that the VCG mechanism is vulnerable to malicious behavior in the case of divisible resource allocation too like in indivisible case proved in [27].

Furthermore, in the malicious case when user i is not in the system, we have

$$Q_k^i = \frac{\alpha_k X_{max}}{\alpha_k + (1+\theta_k) \sum_{j \neq k,i} \alpha_j}, i \neq k, \tag{6.6}$$

$$Q_j^i = \frac{\alpha_j (1+\theta_k) X_{max}}{\alpha_k + (1+\theta_k) \sum_{j \neq k,i} \alpha_j}, \forall j \neq k, i, \tag{6.7}$$

$$Q_j^k = \frac{\alpha_j X_{max}}{\sum_{m \neq k} \alpha_m}. \tag{6.8}$$

By substituting equations (6.4), (6.5), (6.6),(6.7) and (6.8) in (6.3), the VCG payment for the malicious case is

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

$$C_k^{VCGm} = \sum_{j \neq k} \alpha_j \log \left(\frac{\alpha_k + (1+\theta_k) \sum_{m \neq k} \alpha_m}{(1+\theta_k) \sum_{m \neq k} \alpha_m} \right).$$

We observe that the payment of malicious users increases and that of selfish users decreases as θ_k changes from 0 to -1. However, the higher payment is not sufficient to prevent malicious behavior.

6.2 Price of Malice in Mechanisms

We quantify in this section, the resilience of some network mechanisms to malicious behavior. For this purpose, we use the definition of PoM in the Definition 2.21. Now, we proceed to estimate the value of Price of Malice parameter for different network mechanisms. First, we start with the direct VCG mechanism which was shown to be nonresistant to malicious behavior in the previous section.

6.2.1 Price of Malice in VCG Mechanism

The case where user k is malicious and users have logarithmic utility function we could obtain analytical expression for PoM in VCG Mechanism which can be generalized to other cases.

Proposition 6.1. *For the additive resource sharing with user utility functions given in equation (6.2), the Price of Malicious of VCG mechanism $PoM(VCG)$ is*

$$PoM(VCG) = \frac{\sum_{j\neq k} \alpha_j \log\left(\dfrac{\alpha_k + (1+\theta_k)\sum_{j\neq k}\alpha_j}{(1+\theta_k)\sum_m \alpha_m}\right)}{\sum_{j\neq k} \alpha_j \log\left(\dfrac{\alpha_j X_{max}}{\sum_m \alpha_m}\right)}$$

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

$$PoM(VCG) = \frac{\log\left(\frac{N-1+\frac{1}{1+\theta_k}}{N}\right)}{\log\left(\frac{X_{max}}{N}\right)}.$$

Proof. $PoM(VCG)$ is derived directly by substituting the equations (6.7) and (6.6) in Section 6.1.1 to the Definition 2.21 given above. □

We could observe that when the maliciousness of users increase, i.e., as θ decreases from 0 to -1, we can see that the Price of Malice increases. We could observe that the $PoM(VCG)$ can be bounded for different possible values of θ_k and is unbounded when θ_k reaches -1.

6.2.2 Price of Malice in Indirect Auction Mechanisms

Here we present indirect auction mechanisms ([72]) 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. In the indirect mechanisms, instead of reporting their utility function to the designer, the players take a best response to the actions of other players and to the allocation and pricing rules set by the designer. Therefore, the allocation and pricing rules are not a function of utility functions unlike direct VCG mechanism, but rather fixed functions of the player strategies. We consider

indirect auction mechanisms with scalar bid here since they have only one dimensional communication requirement which is suitable for network resource allocation. The malicious behavior considered in this section is that the malicious players take maximum possible share of the resources according to their θ value. This way the malicious players aim to disrupt other players by denying their fair share of resources.

6.2.3 Auctions for Rate Control in Networks

We consider the rate sharing problem with users having separable utility function of their allocation and quantify the effect of the adversarial behavior on it. Let users with utilities $U_i(Q_i)$ share a fixed bandwidth Q_{max} such that $\sum_{i=1}^{N} Q_i(\mathbf{x}) \leq Q_{max}$, where $x_i \in (0, x_m)$. The vector $\mathbf{x}$ in this case denotes player flow rates and $\mathbf{Q}$ the capacity allocated to them ([109, 2]). Consider the utility function given in (2.10) and the cost of i^{th} user is then given by,

$$J_i^m(\mathbf{x}, \theta_i) = C_i(\mathbf{x}) - U_i(Q_i(\mathbf{x})) - \theta_i \sum_{j \in S} U_j(Q_j(\mathbf{x})), \forall i. \tag{6.9}$$

We consider the efficient proportional allocation auction mechanism $\mathscr{M}_a$ introduced in [75] which is an indirect mechanism where the users submit a scalar bid. The proportional allocation which is defined based on the bid vector of players $\mathbf{x}$ is

$$Q_i(\mathbf{x}) := \frac{x_i}{\sum_j x_j + \omega} Q_{max}, \tag{6.10}$$

where ω can be seen as the reserve bid ([57]) and it removes the singularity of the function. For $\omega = 0$, we could see that the resource is completely utilized, i.e., $\sum_i Q_i = Q_{max}$.

We next briefly show how the pricing rule/function is designed with the use of a generator function, as in [75]. In Section 6.5 of this chapter, we detail the procedure with taking into consideration malicious behavior. Let us define $t = \sum_j x_j + \omega$ as 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 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 [75] as

$$C_i(\mathbf{x}) = x_i \sum_{j \neq i} x_j + \omega, \tag{6.11}$$

which is convex payment function in x_i and is sufficient to guarantee a unique Nash equilibrium. We found a mistake in [75], when using $g(t) = t$. The payment function for this case

$$C_i(\mathbf{x}) = \log\left(1 + \frac{x_i}{\sum_{j \neq i} x_j}\right) \sum_{j \neq i} x_j,$$

is concave in x_i and contradicts with the convexity result in Proposition 1 and 2 in [75]. Therefore, we do not use $g(t) = t$.

Being oblivious to the presence of malicious users, the designer employ the same allocation rule and payment to i^{th} user as the one obtained above for mechanism $\mathscr{M}_a$ assuming all the users are just selfish. First, we characterize the modified Nash equilibrium if some of these users are malicious or altruistic. Let us check for the special case of logarithmic utilities and the mechanism $\mathscr{M}_a$.

Proposition 6.2. *The mechanism $\mathscr{M}_a$ defined by (6.10) and (6.11) with users having logarithmic utilities admits several Nash equilibria and one NE point is given as*

$$x_i^* = \frac{\alpha_i}{t(1+\theta_i)Q_{max}}, \tag{6.12}$$

where $-1 < \theta_i \leq \alpha_i(\frac{1}{x_m} + \frac{t}{x_m^2})$.

Proof. For the allocation in (6.10) the strategy space constrained by the set $0 \leq x_i \leq x_m \, \forall i$ satisfy the Assumption 2.1. Then by a standard theorem of game theory (Theorem 4.4, p.176, in [13]), the network game admits a NE.

For the payment given in (6.11), allocation in (6.10) and logarithmic utility function, the cost functions satisfies Assumption 2.4 for $\theta_i < 0$. For altruistic case, i.e. $\theta_i > 0$, the cost functions satisfies Assumption 2.4 only for

$$\theta_i \leq \alpha_i(\frac{1}{x_m} + \frac{t}{x_m^2}).$$

This is obtained by checking for $\frac{d^2 J_i^m}{dx_i^2} \geq 0$. We consider in the game only altruistic users satisfying this condition, in order to obtain an equilibrium. Since the cost function satisfies Assumption 2.4 for all the users with $-1 < \theta_i \leq \alpha_i(\frac{1}{x_m} + \frac{t}{x_m^2})$, the best response points obtained from first order conditions gives a Nash equilibrium.

The best response of user becomes

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

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

□

Remark 6.1. In [94], the conditions for existence of a unique NE for an $N-$person game is given. In addition to Assumption 2.4, the cost functions should satisfy diagonal strict concavity of the weighted nonnegative sum of the cost functions as given in Theorem 2 of [94]. The cost function does not necessarily satisfy this condition in our case. Therefore, the NE is not unique.

We can observe that malicious users having $-1 < \theta < 0$, will have the Nash equilibrium point as $x_i^* > \frac{\alpha_i}{tQ_{max}}$. Therefore, the malicious users bid higher than the selfish users and obtain a disproportionate higher share of resource.

If we use the the modeling in equation (2.13), the Nash equilibrium point of the mechanism $\mathscr{M}_a$ with logarithmic utilities is obtained in similar way as above is

$$x_i^* = \frac{(1-|\theta_i|)\alpha_i}{t(1+\theta_i)X_{max}}. \tag{6.13}$$

We can observe that for malicious users having $-1 < \theta < 0$, the NE point is same as the all selfish case ($x_i^* = \frac{\alpha_i}{tQ_{max}}$), i.e., no malicious effect. But it can be observed that there is a higher effect of altruistic users on selfish users in the case of (6.13) compared to (6.12). For example, with $\theta = 1$, NE point of altruistic user is $x_i^* = \frac{\alpha_i}{2tQ_{max}}$ according to (6.12) but $x_i^* = 0$ according to (6.13), i.e, the altruistic user leaves the entire resource for the selfish users usage. Therefore, modeling in equation (2.13) is useful to capture extreme altruistic behavior.

The allocation for the regular selfish users, i.e., users with $\theta_i = 0$ in the presence of malicious users can be written as

$$Q_i' = \frac{\frac{\alpha_i}{tQ_{max}}Q_{max}}{\sum_{j\in\mathscr{S}}\frac{\alpha_j}{tQ_{max}} + \sum_{k\in\mathscr{B}}\frac{\alpha_k}{t(1+\theta_k)Q_{max}} + \omega}. \tag{6.14}$$

Let

$$r_i = \frac{Q_i}{Q_i'} = \frac{\sum_{j\in\mathscr{S}}\alpha_j + \sum_{k\in\mathscr{B}}\frac{\alpha_k}{(1+\theta_k)} + \omega}{\sum_j \alpha_j + \omega} \tag{6.15}$$

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 $\mathscr{M}_a$ at the NE point given in Proposition 6.2.

Proposition 6.3. *For the additive resource sharing case , the Price of Malicious $PoM(\mathscr{M}_a)$ is*

$$PoM(\mathscr{M}_a) = \frac{\sum_{j\in\mathscr{S}}\alpha_j\log(r_j)}{\sum_{j\in S}\alpha_j\log\left(\frac{\alpha_j Q_{max}}{\sum_i\alpha_i+\omega}\right)}.$$

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

$$PoM(\mathscr{M}_a) = \frac{\log\left(\frac{\alpha(N-1+\frac{1}{1+\theta_k})+\omega}{N\alpha+\omega}\right)}{\log\left(\frac{\alpha Q_{max}}{N\alpha+\omega}\right)}.$$

Proof. The results follow directly by using the allocation given in equation (6.10) and the value of r_i in equation (6.15) to the definition of PoM in Definition 2.21. □

Remark 6.2. We could see that $PoM(\mathscr{M}_a)$ is equal to $PoM(VCG)$ when $\omega = 0$ for the special case of the utility function considered. It is because the proportional allocation coincides with the VCG allocation for this case. But we get very different $PoM(\mathscr{M}_a)$ and $PoM(VCG)$ in the case of the other utility functions, for example $U_i(Q_i) = \alpha_i \log(1+Q_i)$.

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

$$x_i := P_i(\mathbf{x})Q_i(\mathbf{x}), \tag{6.16}$$

the pricing function

$$P_i := \frac{\sum_{j\neq i} x_j + \omega}{Q_{max}}, \tag{6.17}$$

and the resource allocation rule

$$Q_i := \frac{x_i}{\sum_{j\neq i} x_j + \omega} Q_{max}. \tag{6.18}$$

for a scalar $\omega > 0$ sufficiently large such that $\sum_i Q_i \leq Q_{max}$.

Consider now the mechanism $\mathscr{M}'_a$ for the logarithmic case. The cost function in this case is,

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

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

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

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,

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

A Nash equilibrium point could be obtained from the intersection of all these points since the cost function satisfies Assumption 2.4 for $\theta \leq 0$. But it is not possible to have analytical result for the NE in this case. As above in the case of $\mathscr{M}_a$, the PoM can be calculated in this case also but numerically. Therefore, the variation of values of $PoM(\mathscr{M}'_a)$ for different values of θ is given in the simulation section.

Remark 6.3. From the Propositions 6.3 and 6.1, we could 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.

6.2.4 Auctions for Interference Coupled Systems

Consider an auction mechanism in the context of a wireless network and uplink power control setting ([38, 57]) where due to the interference coupling the resource sharing is inherently competitive. Let the user utilities be taken as $U_i(\gamma_i(\mathbf{Q}))$ and the individual power levels, Q, satisfy $\sum_{i=1}^{N} Q_i \leq Q_{max}$, where the SINR received by the base station is given in equation (6.1). We propose an auction-based mechanism $\mathscr{M}_b$, defined by equations (6.11) and (6.10) with $\omega = 0$ for interference coupled systems.

Proposition 6.4. *The auction-based mechanism, $\mathscr{M}_b$, is an ϵ-efficient mechanism for system having users with interference coupled utility functions $U_i(\gamma_i(\mathbf{Q})$ if*

$$\frac{|U_i''|}{U_i}(\gamma_i + L) > 2. \tag{6.19}$$

Proof. We decouple the user utilities by rewriting γ_i as

$$\gamma_i(Q_i) = \frac{Q_i(\mathbf{x})}{Q_{max} - Q_i(\mathbf{x}) + \sigma}, \tag{6.20}$$

using the full utilization property of the mechanism $\mathscr{M}_a$ when $\omega = 0$.

In [57], it is observed that in systems with sufficiently high SINR satisfying the Assumption 2 given in equation (6.19)

$$U_i(\gamma_i(Q_i)) = U_i(\frac{Q_i}{Q_{max} - Q_i + \sigma})$$

is concave in Q_i. It can be also seen that $U_i(\gamma_i(Q_i))$ is monotonically increasing and twice differentiable in Q_i. Therefore, the sufficient condition for the existence of an ϵ-efficient unique NE is satisfied along with allocation given in (6.11) and pricing given in (6.10).

□

For the allocation given in (6.10), the SINR at NE point $\mathbf{x}^*$ is

$$\gamma_i(\mathbf{x}^*) = \frac{x_i^* Q_{max}}{\sum_j x_j^*(Q_{max} + \sigma) - x_i^* Q_{max}}. \tag{6.21}$$

In the presence of malicious and altruistic users, let the SINR obtained by the regular users be $\gamma_i(\mathbf{x}')$ where $\mathbf{x}'$ is the new NE point. Now we give the value of $PoM(\mathscr{M}_b)$ in the following proposition for the interference coupled wireless system.

Proposition 6.5. *The PoM of the mechanism $\mathscr{M}_b$ for the interference coupled wireless system is given as*

$$PoM(\mathscr{M}_b) = \frac{\sum_{j \in \mathscr{S}} \alpha_j \log(\frac{\gamma_j(\mathbf{x}^*)}{\gamma_j(\mathbf{x}')})}{\sum_{j \in \mathbf{S}} \alpha_j \log(\gamma_j(\mathbf{x}^*))}.$$

where $\mathbf{x}'$ and $\mathbf{x}^*$ are the NE points with and without the presence of malicious users.

The numerical results for variation of $PoM(\mathscr{M}_b)$ for the interference coupled wireless system is given in the simulation section for a specific set of wireless system parameters for different values of θ.

6.2.5 Price of Malice in Pricing Mechanisms

In pricing mechanisms the users choose their allocation as their strategy or action. Pricing mechanisms do not have explicit allocation rule. 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 2.21 for pricing mechanisms, which differ from auctions by their lack of an explicit resource allocation scheme, can be obtained by replacing $Q(\mathbf{x})$ and $Q(\mathbf{x}')$ with the action vector without malicious users $\mathbf{x}$ and with malicious users $\mathbf{x}'$, 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 $\sum_{i=1}^{N} x_i = X_{max}$, and $x_i \in (0, x_m)$. Consider an efficient mechanism $\mathscr{M}_c$, for which the efficient allocation is

$$x_i = \frac{\alpha_i}{\lambda}, \tag{6.22}$$

where λ is the Lagrange multiplier. In the case of all selfish users $\lambda = \sum_i \alpha_i / X_{max}$ 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,

$$J_i^m(\mathbf{x}, \theta_i) = P_i x_i - U_i(x_i) - \theta_i \sum_{j \in S} U_j(x_j). \tag{6.23}$$

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 should be less than 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 $\lambda = \sum_i \alpha_i / X_{max}$. The remaining resource $(X_{max} - \sum_B x_m)$ will be shared among good users, under the efficient mechanism $\mathscr{M}_c$, i.e., $x_i = \frac{\alpha_i}{\lambda'}$.

Proposition 6.6. *In the additive sharing case $PoM(\mathscr{M}_c)$ is,*

$$PoM(\mathscr{M}_c) = \frac{\sum_{j \in \mathscr{S}} \alpha_j \log\left(\frac{X_{max}\lambda'}{\sum_i \alpha_i}\right)}{\sum_{j \in \mathscr{S}} \alpha_j \log\left(\frac{\alpha_j X_{max}}{\sum_i \alpha_i}\right)}.$$

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

$$PoM(\mathscr{M}_c) = \frac{\log\left(\frac{X_{max}\lambda'}{N\alpha}\right)}{\log(\frac{X_{max}}{N})}.$$

Remark 6.4. For the interference-coupled case, pricing mechanism is proposed in Chapter 3. Let us denote the mechanism as $\mathscr{M}_d$ for the interference-coupled case. In the mechanism $\mathscr{M}_d$, the price is not the same for all the users as Lagrange multiplier unlike $\mathscr{M}_c$. Discriminated prices are obtained for the users which as functions of channel parameters and received SINRs, as a result of interference-coupling.

6.3 Additional metrics to quantify the effect of malicious behavior

Our *PoM* definition is similar to the externality-price definitions in [6] in the context of altruistic behavior, since we quantify the effect of malicious players on selfish players. Now we introduce additional metric definitions to quantify the effect of malicious behavior.

6.3.1 Maliciousness Price

Here we first define and quantify maliciousness price based on social welfare of all the players including malicious ones.

Definition 6.7 (Social Maliciousness Price(SMP))**.** The ratio between the social welfare of players, at equilibrium before and after the presence of malicious players.

$$SMP(\mathscr{M}) := \frac{\sum_{j\in\mathscr{A}} U_j(Q'_j(\mathbf{x}'))}{\sum_{j\in\mathscr{A}} U_j(Q_j\mathbf{x}))}, \tag{6.24}$$

Consider mechanism $\mathscr{M}_a$ and the special case and the additive sharing case with logarithmic utilities with $\omega = 0$. Now we give the Social Maliciousness Price of the mechanism $\mathscr{M}_a$ which is proposed for additive rate sharing in the subsection 6.2.2 above.

Proposition 6.8. *In the additive sharing case $SMP(\mathscr{M}_a)$ is,*

$$SMP(\mathscr{M}_a) = \frac{SW^m}{\sum_{j\in\mathscr{A}} \alpha_j \log\left(\frac{\alpha_j X_{max}}{\sum_i \alpha_i}\right)},$$

where

$$SW^m = \sum_{j\in\mathscr{S}} \alpha_j \log\left(\frac{\alpha_j X_{max}}{\sum_{j\in\mathscr{B}} \alpha_j + \sum_{k\in\mathscr{S}} \frac{\alpha_k}{(1+\theta_k)}}\right) + \sum_{k\in\mathscr{B}} \alpha_k \log\left(\frac{\frac{\alpha_k}{(1+\theta_k)} X_{max}}{\sum_{j\in\mathscr{S}} \alpha_j + \sum_{k\in\mathscr{B}} \frac{\alpha_k}{(1+\theta_k)}}\right).$$

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

$$SMP(\mathscr{M}_a) = \frac{\alpha \log\left(\frac{(1+\theta_k)^{N-1} X_{max}^N}{((N-1)(1+\theta_k)+1)^N}\right)}{\alpha \log\left(\frac{X_{max}^N}{N^N}\right)}.$$

Proof. From equation (6.12), the allocation for malicious users and social welfare with the presence of malicious users in the set $\mathscr{B}$ would be:

$$Q'_k = \frac{\frac{\alpha_k}{t(1+\theta_k)X_{max}} X_{max}}{\sum_{j\in\mathscr{S}} \frac{\alpha_j}{tX_{max}} + \sum_{k\in\mathscr{B}} \frac{\alpha_k}{t(1+\theta_k)X_{max}}}, \tag{6.25}$$

$$SW^m = \sum_{j\in\mathscr{S}} \alpha_j \log\left(\frac{\alpha_j X_{max}}{\sum_{j\in\mathscr{S}} \alpha_j + \sum_{k\in\mathscr{B}} \frac{\alpha_k}{(1+\theta_k}}\right) + \sum_{k\in\mathscr{B}} \alpha_k \log\left(\frac{\frac{\alpha_k}{(1+\theta_k)} X_{max}}{\sum_{j\in\mathscr{S}} \alpha_j + \sum_{k\in\mathscr{B}} \frac{\alpha_k}{(1+\theta_k)}}\right). \tag{6.26}$$

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

$$SW^m = \alpha \log\left(\frac{(1+\theta_k)^{N-1} X_{max}^N}{((N-1)(1+\theta_k)+1)^N}\right). \tag{6.27}$$

The social welfare with all selfish users from (6.10) is

$$SW = \sum_{j\in\mathscr{S}} \alpha_j \log\left(\frac{\alpha_j X_{max}}{\sum_{j\in\mathscr{S}} \alpha_j}\right), \tag{6.28}$$

and for symmetric case

$$SW = \alpha \log\left(\frac{X_{max}^N}{N^N}\right). \tag{6.29}$$

The value of $SMP(\mathscr{M}_a)$ can be obtained directly by substituting (6.26) and (6.28) in (6.24). For the symmetric case, by substituting (6.27) and (6.29) in (6.24). □

Remark 6.5. For the symmetric case, it can be observed that 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. Also, the paradox is obtained for the specific case and may not be true in general.

Now we define another metric to quantify the malicious behavior.

Definition 6.9 (Individual Maliciousness Price(IMP))**.** The ratio between the total utility of malicious players at equilibrium, before and after they become malicious players.

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

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.

6.4 Collusion behavior in Network Mechanisms

Some of the 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 the selfish players to cheat the designer. In this section, we investigate group strategy-proofness of a particular mechanism. Price of Collusion quantifies the effect of collusion on the malicious players in a mechanism. In this section, Price of Collusion and related metrics are also defined to quantify the effect of collusion and expressions are obtained for some of them. This section follows the same framework as given in the Section 2.1.1, with all the users having $\theta = 0$ for equation (2.10) in Subsection 6.4.1 and the users in collusion having $\theta < 0$ for equation (2.10) in Subsection 6.4.2.

6.4.1 Group Strategy-proofness of Mechanisms

We assume here that all the users are selfish who are interested only about their individual utility but by forming the coalition they try to punish the other non-colluding users without any individual utility loss. The group-strategyproof property checks the resistance of a mechanism to collusion tendency of the kind of users who reduce the resource share of non-colluding users but care also about their self utility. We consider the collusion behavior of malicious users in the next subsection.

First, we formally define group strategy-proofness of a mechanism.

Definition 6.10 (Group Strategy-proofness)**.** A mechanism is group strategy-proof if individual players do not gain anything by making a coalition among them and misreporting their true values, i.e.

$$J_k(x_1, ..., x_K, x_{-O}) \leq \tilde{J}_k(\tilde{x}_1, ..., \tilde{x}_K, x_{-O}),\ \forall\ k = 1, ..., K \in O, \tilde{x}_k \in X_k, x_{-O} \in \mathscr{X}_{-O}.$$

where O is the set of players who formed coalition, $\mathbf{x}$ is the original values, $\tilde{x}_k$ is the "misrepresented" value and X_{-O} is the action set of regular players who do not join the coalition.

If a mechanism is not group strategy-proofness it can still be ϵ-group strategy-proof which is defined as follows.

Definition 6.11 (ϵ-Group Strategy-proofness)**.** A mechanism is ϵ-group strategy-proof if,

$$J_k(x_1, ..., x_K, x_{-O}) - \tilde{J}_k(\tilde{x}_1, ..., \tilde{x}_K, x_{-O}) \leq \epsilon,\ \forall\ k = 1, ..., K \in O, \tilde{x}_k \in X_k, x_{-O} \in \mathscr{X}_{-O}$$

and $\epsilon > 0$.

We analyze group strategy-proofness of the approximately efficient and strategy-proof mechanism $\mathscr{M}_a'$ defined above by equations (5.20) and (5.21) in Section 6.2.

Theorem 6.12. *The mechanism $\mathscr{M}_a'$ is resistant to overbidding by a coalition and is ϵ-group strategy-proof where*

$$\epsilon = \max_{k \in \mathscr{O}} \alpha_k \left(\frac{\tau_k^2 - \tau_k^3}{\tau_k^2 - \tau_k + 1}\right), \tag{6.30}$$

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

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

Proof. Consider m adversarial users out of N total form a coalition $\mathscr{O}$ to cheat the system and get higher share of resources together. Let us assume that these agents bid higher than their best response together and the bid from these agents be $\tilde{x}_k = x_k + \delta$ where $-x_k \leq \delta \leq \infty$. Now the allocation for the colluding users will be,

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

and others will be

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

We obtain costs for the colluding users as,

$$\tilde{J}_k = x_k + \delta - \alpha_k \log \left(\frac{x_k + \delta}{\sum_{j \neq k} x_j + (m-1)\delta + \omega} X_{max} \right) \ \forall \ k \in \mathscr{O}.$$

The condition for ϵ-group strategy-proofness is

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

$$\begin{aligned} J_k - \tilde{J}_k &= \alpha_k \log \left(\frac{x_k}{\sum_{j \neq k} x_j + \omega} X_{max} \right) \\ &- \delta + \alpha_k \log \left(\frac{x_k + \delta}{\sum_{j \neq k} x_j + (m-1)\delta + \omega} X_{max} \right) \\ &\leq \epsilon, \ \forall \ k \in \mathscr{O}. \end{aligned} \tag{6.31}$$

This will result in the following inequality given as,

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

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

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

If this condition is satisfied for $\epsilon = 0$, the mechanism is group strategyproof.

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 $\mu > 0$, $\epsilon = 0$. Therefore, the mechanism is group strategyproof for overbidding, i.e., $\delta > 0$.

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,

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

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

Hence proved. □

6.4.2 Price of Collusion of Mechanisms

We didn't quantify the effect of collusion on the network games and mechanisms with malicious users, we checked only if they are resistant to collusion of the selfish users in Section 6.4.1. If a mechanism is group strategyproof, when the malicious users form a collusion and bid higher individually they loose individually if they are considered selfish as from the Definition 6.10. But the malicious users might still form collusion to gain individually according to their modified utility function in (2.10) and as a group reducing the share of resource to the other regular users outside collusion. Here we define and calculate metrics to quantify the effect of collusion in network mechanisms which can be group strategy-proof or not in the presence of malicious colluding users.

In [54], the Price of Collusion defined for any game G is at most the maximum price of anarchy of $G(O)$ over all coalitions O. In other words, it is the worst possible ratio between the social cost at equilibrium before and after the collusion scenario. The PoC defined in [54] will be redefined for our framework now.

Definition 6.13 (Price of Collusion)**.** Price of Collusion of a mechanism is defined as

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

where Q_j^c is the allocation after the collusion formation.

Now we quantify the PoC of the mechanism $\mathscr{M}_a$ defined in Section 6.2.2.

Proposition 6.14. *Price of Collusion of the mechanism $\mathscr{M}_a$ is given by*

$$PoC(\mathscr{M}_a) := \max_{O} \frac{\sum_{k\in O} \alpha_k \log\left(\frac{\alpha_k+\delta}{\sum_{j\in A}\alpha_j+m\delta+\omega} X_{max}\right) + \sum_{i\in S} \alpha_i \log\left(\frac{\alpha_i}{\sum_{j\in A}\alpha_j+m\delta+\omega} X_{max}\right)}{\sum_{k\in A} \alpha_k \log\left(\frac{\alpha_k X_{max}}{\sum_j \alpha_j+\omega}\right)}. \tag{6.32}$$

Proof. Consider m adversarial users out of N total form a coalition O to cheat the mechanism $\mathscr{M}_a$. Let us take that the bid from these agents be $\tilde{x}_k = \alpha_k + \delta$. Now the allocation of the users in the presence of the coalition according to (6.10) will be,

$$Q_k^c = \frac{\alpha_k+\delta}{\sum_{j\in A}\alpha_j + m\delta + \omega} X_{max},\ \forall\ k \in O$$

and

$$Q_i^c = \frac{\alpha_i}{\sum_{j\in A}\alpha_j + m\delta + \omega} X_{max},\ \forall\ i \in S.$$

The utility obtained by each user in the collusion is,

$$U_k(Q_k^c) = \alpha_k \log\left(\frac{\alpha_k+\delta}{\sum_{j\in A}\alpha_j + m\delta + \omega} X_{max})\right)\ \forall\ k \in O. \tag{6.33}$$

From this result we could obtain Price of Collusion of the mechanism $\mathscr{M}_a$ using the Definition 6.13 above. □

In addition, we consider other metrics to quantify the effect of collusion on the set of colluding users and regular users, similar to the different Collusion Prices defined in [6].

Definition 6.15 (Collusion Externality Price (CEP))**.** Collusion externality price is defined as the worst possible ratio between the total cost of players who collude at equilibrium before and after the collusion scenario.

$$CEP(\mathscr{M}) := \max_{O} \frac{\sum_{j\in S} U_j(Q_j^c(x))}{\sum_{j\in S} U_j(Q_j(x))},$$

Definition 6.16 (Individual Collusion Price (ICP))**.** Individual collusion price is defined as the worst possible ratio between the total cost of players who collude at equilibrium before and after the collusion scenario.

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

Remark 6.6. These metrics are similar to the PoM related metrics in Section 6.2 . But collusion is a different malicious behavior since they act together for the total utility of the collusion, for maximum possible harm to the non-colluding users and for their own individual utilities. The malicious users optimize over possible coalitions and find the best coalition in terms of size, members and δ. Therefore, the PoC related metrics are defined as the maximum over possible coalitions.

Using the equation (6.33) above, we could also directly calculate the $ICP(\mathscr{M}_a)$.

Proposition 6.17. *Individual collusion price of the mechanism $\mathscr{M}_a$ is given by*

$$ICP(\mathscr{M}_a) := \max_{O} \frac{\sum_{k\in O} \alpha_k \log\left(\frac{\alpha_k+\delta}{\sum_j \alpha_j + m\delta + \omega} X_{max}\right)}{\sum_{k\in O} \alpha_k \log\left(\frac{\alpha_k X_{max}}{\sum_j \alpha_j + \omega}\right)}. \tag{6.34}$$

6.5 Auctions Resistant to Malicious Users

The robustness analyses of mechanisms and quantification of PoM in the Section 6.2 only measure the effect of malicious users but does not provide a way to encounter them. In [87] it was shown that the Second Price auction can be made robust to interdependent preferences corresponding to altruistic or malicious behavior by changing just the pricing to that of a First Price auction, augmented by bonus payments. Similar to this approach, in this section we consider a possible response schemes to adversarial behavior, based on a softer punishment scheme using differentiated pricing.

6.5.1 Differentiated Pricing

We propose 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 [3]. The response mechanism is implemented by the designer by deploying a differentiated pricing. First, we define a trade-off metric $T(\mathscr{M})$ for quantifying the vulnerability of a pricing-based response to a mechanism $\mathscr{M}$. 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 6.18. A metric for quantifying vulnerability of a pricing-based response mechanism against a set of malicious users $B \subset A$ is defined as:

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

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.

6.5.2 Auctions for Additive Sharing

We consider the network mechanism $\mathscr{M}_a$ proposed for network rate sharing in Section 6.2.2 and modify it with a new payment function. We propose now a differentiated payment function to counter the malicious behavior of users and propose a new mechanism using this payment function. We first assume 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. We propose mechanism $\mathscr{M}_m$ in the following proposition which is efficient in the presence of malicious users, i.e., $PoM(\mathscr{M}_m) = 1$.

Proposition 6.19. *The mechanism $\mathscr{M}_m$ defined by the allocation in (6.10) with $\omega = 0$ and the payment*

$$C_i(\mathbf{x}) = x_i \sum_{j\neq i} x_j - \theta_i(N-1)tX_{max} \log\left(1 + \frac{x_i}{\sum_{j\neq i} x_j}\right), \tag{6.35}$$

is efficient in the presence of malicious users and makes the malicious user take the strategy $x_i^* = \dfrac{\alpha_i}{tX_{max}}$ for network rate sharing with users having logarithmic utility functions.

Proof. The cost function of users from equation (6.9) for the proportional allocation given in (6.10) with $\omega = 0$ and logarithmic utility function is

$$J_i^m(\mathbf{x}) = C_i(\mathbf{x}) - \alpha_i \log\left(\frac{x_i}{\sum_k x_k}\right) - \theta_i \sum_{j \neq i} \alpha_j \log\left(\frac{x_j}{\sum_k x_k}\right), \forall i. \tag{6.36}$$

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

$$\frac{\partial J_i^m}{\partial x_i} = \frac{\partial C_i}{\partial x_i} - \frac{\partial U_i}{\partial Q_i} \frac{\sum_{j \neq i} x_j}{(\sum_k x_k)^2} + \theta_i \sum_{j \neq i} \frac{\alpha_j}{x_j \sum_k x_k} = 0. \tag{6.37}$$

This gives,,

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

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

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

Doing the substitutions,

$$\begin{aligned} \frac{\partial U_i(Q_i)}{\partial Q_i} &= \frac{t}{1 - \dfrac{Q_i}{X_{max}}} \left(\frac{\partial C_i(Q_i, t)}{\partial x_i} + \theta_i \sum_{j \neq i} \frac{1}{t}\right) \\ &:= f(Q_i, t). \end{aligned} \tag{6.38}$$

The designer should solve the constrained optimization problem

$$\max_{\mathbf{Q}} V(\mathbf{Q}) \Leftrightarrow \max_{\mathbf{Q}} \sum_i U_i(Q_i) \text{ such that } \sum_i Q_i = Q_{max}, \tag{6.39}$$

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

$$L(\mathbf{Q}) = \sum_i U_i(Q_i) + \lambda \left(Q_{max} - \sum_i Q_i\right),$$

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

$$\frac{\partial L}{\partial Q_i} \Rightarrow U_i'(Q_i) = \lambda, \ \forall i \in A, \tag{6.40}$$

and the efficiency constraint

$$\frac{\partial L}{\partial \lambda} \Rightarrow \sum_i Q_i = Q_{max}. \tag{6.41}$$

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

When we compare (6.38) and (6.40), 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 [75]. For this we make $f(Q_i, t)$ independent of Q_i and derive the 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

$$C_i(\mathbf{x}) = \int_0^{x_i} \frac{g(s + \sum_{j\neq i} x_j)}{(s + \sum_{j\neq i} x_j)^2} ds \sum_{j\neq i} x_j - \theta_i \int_0^{x_i} \frac{ds}{s + \sum_{k\neq j} x_k} \sum_{j\neq i} \frac{\alpha_j}{x_j}. \tag{6.42}$$

For $g(t) = t^2$, we obtain

$$C_i(\mathbf{x}) = x_i \sum_{j\neq i} x_j - \theta_i \log\left(1 + \frac{x_i}{\sum_{j\neq i} x_j}\right) \sum_{j\neq i} \frac{\alpha_j}{x_j}. \tag{6.43}$$

Let us assume that the users except i^{th} user are merely selfish due to the payment function of the mechanism they report $x_i = \dfrac{\alpha_i}{tX_{max}}$. Then, we obtain (6.35) as the payment function which corresponds to the efficient allocation. If the malicious user takes best response using the payment (6.35) in (6.9), the best response is obtained as $x_i = \dfrac{\alpha_i}{tX_{max}}$. □

Remark 6.7. If the designer punishes the users who are detected as malicious with a payment in which $\theta_i = -1$, without knowing the exact θ value in a more realistic situation, the pricing function becomes

$$C_i(\mathbf{x}) = x_i \sum_{j\neq i} x_j + \log\left(1 + \frac{x_i}{\sum_{j\neq i} x_j}\right)(N-1). \tag{6.44}$$

For this cost function to be convex, in order to take the best response, from the second order conditions we get

$$N \leq \frac{\sum_{j\neq i} \alpha_j}{Q_{max}^2} + 1.$$

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 as in (6.44). Even if the cost function is not convex, it 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 (6.11) which is convex.

The tradeoff-parameter of mechanism $\mathscr{M}_m$ is given by,

$$T(\mathscr{M}_m) \geq \frac{\sum_{j\in S} \alpha_j \log(r_j)}{\sum_{i\in B} x_i \sum_{j\neq i} x_j + \log\left(1 + \frac{x_i}{\sum_{j\neq i} x_j}\right)(N-1)}.$$

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.

6.5.3 Differentiated Pricing 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. 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 $\mathscr{M}_e$, which is a modified version of $\mathscr{M}_c$. 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, $T(\mathscr{M}_e)$ is obtained as,

$$T(\mathscr{M}_e) \geq \frac{\sum_{j\in S}\alpha_j \log\left(\frac{X_{max}\lambda'}{\sum_i \alpha_i}\right)}{\sum_{i\in B} e^{\kappa_i(x_i-(\overline{x}+\epsilon))}}.$$

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

$$T(\mathscr{M}_e) \geq \frac{\log\left(\frac{X_{max}\lambda'}{N\alpha}\right)}{e^{\kappa_i(x_i-(\overline{x}+\epsilon))}}.$$

6.5.4 Differentiated Pricing for Interference Coupled Systems

Consider the case of pricing in interference coupled systems given in Section 6.2.5. To counter the malicious behavior, the designer introduces a new mechanism $\mathscr{M}_f$ 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 [5, 18]. For the mechanism $\mathscr{M}_f$, the trade-off metric $T(\mathscr{M}_f)$ can be obtained in similar way as for additive sharing case. The variation of values of $T(\mathscr{M}_e)$ and $T(\mathscr{M}_f)$ for different number of users is given and compared with each other in the simulation section.

6.6 Simulations

In this section, computer simulation results are presented to show the different parameters of the proposed mechanisms.

First, the Price of Malice $PoM(\mathscr{M}_a)$ and $PoM(\mathscr{M}_b)$ of auction mechanism for additive sharing $\mathscr{M}_a$ and interference coupling $\mathscr{M}_b$, is plotted, using the setup in Section 6.2 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 $X_{max} = 30$ 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 6.1. It can be observed that value of $PoM(\mathscr{M}_a)$ and $PoM(\mathscr{M}_b)$ decreases as θ varies from -1 to 0 as expected.

We next compute the Price of Malice $PoM(\mathscr{M}'_c)$ and $PoM(\mathscr{M}'_d)$ for the pricing mechanism for additive sharing $\mathscr{M}'_c$ and interference coupling $\mathscr{M}'_d$ respectively, by varying the number of users from 8 to 15. The simulations are done by generating the player

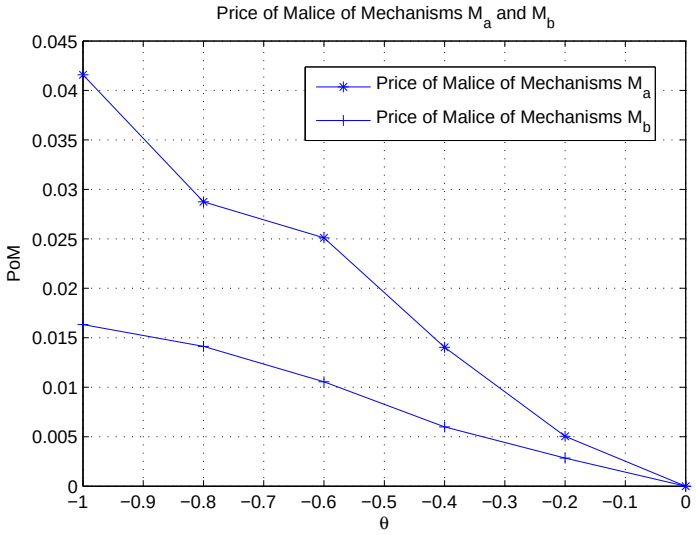

Figure 6.1: Price of Malice $PoM(\mathscr{M})$ of the auction mechanism for additive coupling $\mathscr{M}_a$ and interference coupling $\mathscr{M}_b$ in Section 6.2.2 for varying values of θ.

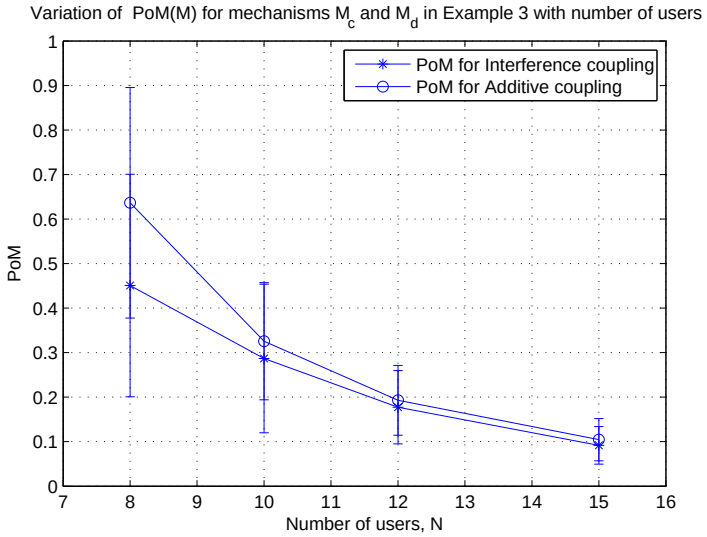

Figure 6.2: Price of Malice $PoM(\mathscr{M})$ of the pricing mechanisms for additive coupling $\mathscr{M}'_c$ and interference coupling $\mathscr{M}'_d$ for varying number of users.

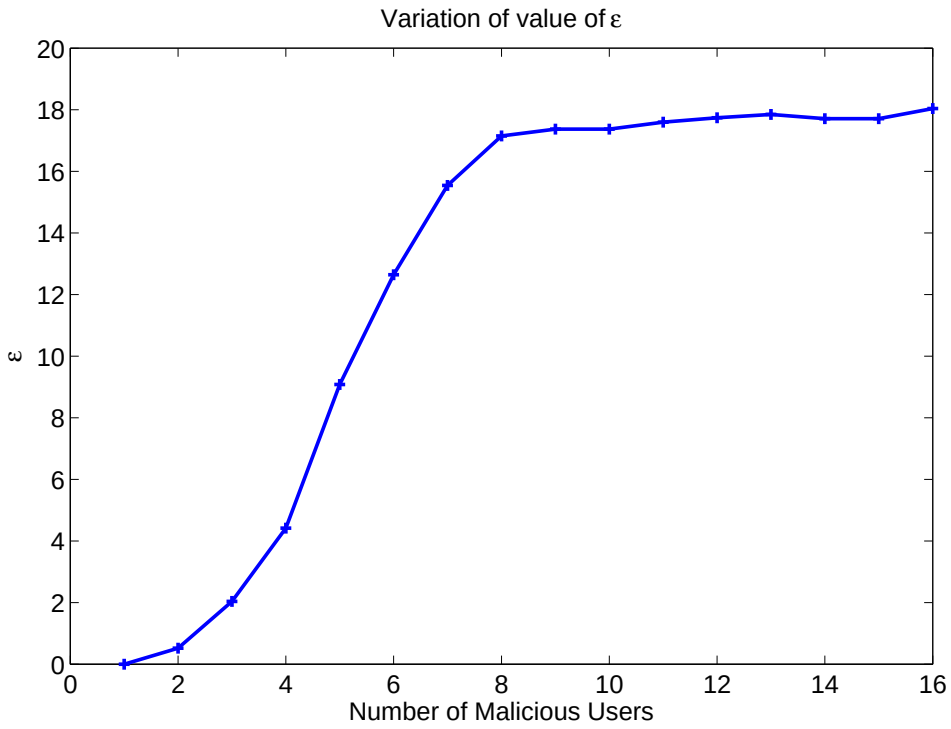

Figure 6.3: Variation of value of ϵ with number of malicious users for the ϵ-group strategyproof mechanism $\mathscr{M}'_a$ in Section 6.4.1.

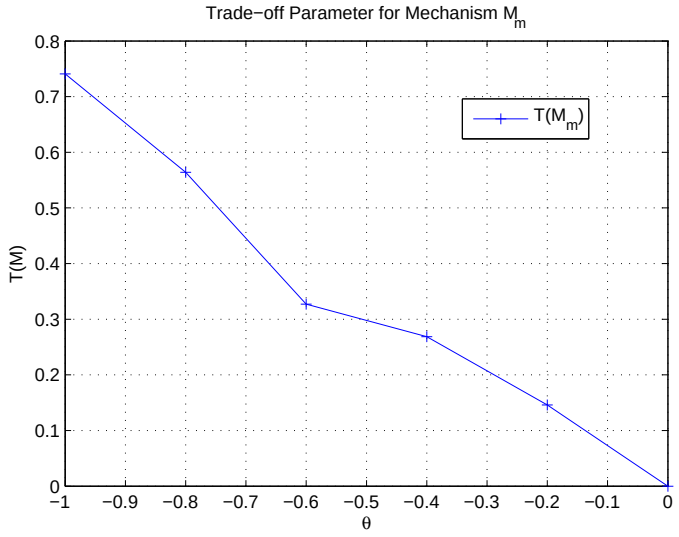

Figure 6.4: Trade off parameter $T(\mathscr{M})$ of auction mechanism $\mathscr{M}_m$ with differentiated pricing for additive sharing given in Section 6.5 for varying values of θ.

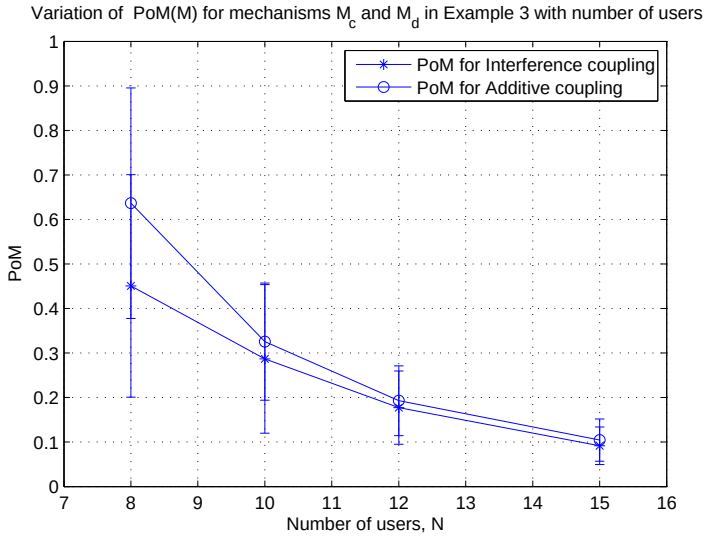

Figure 6.5: Trade off parameter $T(\mathscr{M})$ of pricing mechanisms for additive coupling $\mathscr{M}_e$ and interference coupling $\mathscr{M}_f$ given in Section 6.5 with varying number of users.

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 $PoM(\mathscr{M})$ values are plotted in Figure 6.2. The number of malicious users is fixed at 3, $X_{max} = 5$, $\sigma = 0.5$ 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 $PoM(\mathscr{M}'_c)$ and $PoM(\mathscr{M}'_d)$ are plotted in Figure 6.2. 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 $\mathscr{M}'_a$ is simulated. The variation of value of ϵ defined in (6.30) with number of malicious users for the mechanism $\mathscr{M}'_a$ is plotted in Figure 6.3. 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 $T(\mathscr{M})$ is plotted for auction mechanism $\mathscr{M}_m$ in Section 6.5 for additive sharing for different values of θ in Figure 6.4. The users having $x > \overline{x} + 2\ \sigma_x$ are priced differentially as described in Section 6.5.

Finally, the trade-off parameter $T(\mathscr{M})$ is plotted for pricing mechanisms $\mathscr{M}_e$ and $\mathscr{M}_f$ given in Section 6.5, in Figure 6.5. An iterative algorithm as given in [18] is used to obtain allocation and prices. The other parameters remain the same as those used to generate the Figure 6.2. It can be seen from Figure 6.5 that mechanism $\mathscr{M}_f$ performs better than $\mathscr{M}_e$ in this case, possibly due to the coupling involved.

6.7 Conclusion

In this chapter first we have showed the efficiency loss in VCG mechanism for allocation of divisible resources, in the presence of malicious users. Then we calculated the NE of different indirect mechanisms with malicious users for wireline and interference limited wireless networks. The PoMs for different mechanisms are calculated at these NEs, also for the symmetric case. In the interference coupled case, PoMs of different mechanisms have been observed to be unbounded for different values of degree of parameter. The additional price for the malicious users compared to the regular users has been observed to be proportional to their respective degree of maliciousness.

7 Bayesian Mechanisms and Detection Methods for Wireless Network Security

7.1 Introduction

In this chapter, we model malicious users in an ad-hoc wireless network, where compromised devices act like regular (selfish) users accepting the mechanism rules, which are the prices and allocation determined by the network (designer). This way, they avoid immediate detection and continue having access to resources such as transmission power and spectrum. The legitimate users and the designer know only the probability with which a mobile device could be a bot and study the effect of this scenario on the wireless network (mechanism). The observation of the network over a long period of time gives the designer and the regular users probabilistic information about malicious behavior of some of the users.

In the mechanisms under consideration, the users are also uncertain about the nature of other users, i.e. whether others are regular users or bots (malicious users). In this chapter, we study the conditions under which uncertainty in the network is beneficial for regular users. The boundary conditions are based on wireless system parameters. A malicious user does not want to harm other malicious users by unnecessarily spending more energy and paying more price for the extra power. Therefore, by creating the uncertainty about their nature by hiding, the regular users confuse the malicious users. The uncertainty created in the network is a way for the regular users to counter the malicious users and have better utility for themselves. *Windfall of malice* [95] is a paradoxical situation in which the presence of the malicious user becomes beneficial for the regular users. This is achieved in some situations due to the lack of information in the network about the nature of users, compared to the case where all the users are regular. Windfall of malice can be also achieved by pricing the malicious user comparatively very high compared to the regular users.

We consider Jamming [99] which is a Denial of Service (DoS) attack on the Medium Access (MAC) of a power controlled wireless network. In a distributed power controlled network, where every user selects its own transmitting power, the regular users maximize their SINR subject to energy constraint. The jammers, even at the expense of their energy spending, creates interference to other regular transmitters.

In [98], Bayesian jamming games are considered and the NE points for different jamming scenarios are obtained. Unlike the work in [98], we propose a mechanism design framework for pricing mechanisms and auctions[35] in the presence of malicious users (bots) and modify the mechanisms to counter malicious behavior. Our model captures the fact that, in addition to the resource allocation the malicious users affect the regular

users through the prices charged to the users. In the scenario considered in this chapter, bots hide among the crowd of regular users accepting the prices and allocations from the designer, but use resources for their purpose and harm others. Unlike in [98], we consider a more realistic setting where none of the users have incentive to reveal their nature. This is also important in the botnet setting we consider in this thesis. We find the conditions under which the incomplete information in the network is beneficial for the users and designer, by comparing the incomplete information case to the complete information case. We extend the Kelly mechanism given in [70] for interference coupled networks in the presence of users with unknown nature and obtain the prices. We also analyze the effect of uncertainty about the presence of malicious users in auction mechanisms and modify them to counter the scenario. Truthfully implementable mechanism in Nash equilibrium where the base station elicits truthful signals from the noncooperative mobiles is proposed in [68]. Truthful mechanisms for wireless ad-hoc networks is also proposed in [91]. We study truthful Bayesian mechanisms for the wireless network scenario in Section 7.7 and quantify the effect of malicious users.

Anomaly-based detection techniques try to detect bots based on network traffic anomalies such as high network latency, high volumes of traffic, traffic on unusual channels, and unusual network behavior that could indicate the presence of malicious bots in the network [44]. Our detection technique to detect bots, using the prices corresponding to unusual network traffic with a pattern, falls under the class of anomaly-based detection techniques. We employ Bayesian hypothesis testing[89] or a machine learning based technique for existence of a bot [50], in the network layer. In [89], a decentralized Bayesian detection for sensor networks is analyzed. There are N sensors which perform decentralized hypothesis testing to check if another user is a regular user or bot.

We analyze Bayesian mechanisms [48] which have a designer (network) who designs allocation and prices based on information expressed as a probabilistic distribution over the type of the users. The utility a user derives is a function of the Signal-to-Interference plus Noise Ratio (SINR) which is a Quality of Service (QoS) metric in wireless network. The impact of the malicious behavior in interference limited wireless network is quantified within a Bayesian framework and malicious behavior resistant mechanisms are designed. We analyze an incomplete information case where the malicious behavior is countered without explicit detection of malicious users or learning their nature. The designer knows the probability of malicious user's existence and counters them by updating the prices using the probabilistic information. The additional pricing by the designer and the hiding strategy of the regular users in the pricing mechanism counter malicious activities. The pricing is given such that the BR power converges to achieve the QoS requirement of each user and the malicious behavior of the users is prevented.

In addition to well known jamming or denial-of-service attacks, an emerging scenario is when the mobile devices such as tablets or smart phones are used as bots by a malicious agent (botmaster). Botnets[124] are software programs which compromise the networked devices (bots) and carry out Distributed Denial of Service (DDoS) attacks in the network. DDoS attacks use the overall network bandwidth and other resources of the bots, to deny the legitimate access to resources. The high inter-connectivity of the wireless network with the Internet makes these networks highly vulnerable to botnet attacks. A small

number of mobiles can be used as bots to geo-locate majority of users in the network during significant fraction of the users travel with their devices[62]. We consider Botnets as a specific instance of the general wireless network security problem, which we consider in this chapter, and numerical analysis is carried out with real Botnet data.

7.2 Bayesian Mechanism Model

First, we give the model of the mechanism with an arbitrary number of regular and malicious users. Let $\mu^m(N, N^m)$ and $\mu^s(N, N^m)$ be the joint probability mass function (pmf) of N and N^m as observed by malicious and regular user respectively. The users do not know the nature of the users around them and evaluate their costs based on the pmfs. In addition to the price, the users have battery energy cost for transmission in the uplink of a wireless link. Let a user spends energy B for transmission per unit of transmit power.

The cost function of the regular user will be,

$$J_i^s(x^s, x^m) = C_i^s(\mathbf{x}) + B\frac{x_i^s}{h_i} - \sum_{N^m=0}^{N} \mu^s(N, N^m)U(\gamma_i^s(N, N^m)). \tag{7.1}$$

For the symmetric case, when the channel gains of all the regular users and malicious users are equal to h^s and h^m respectively, the SINR of regular users become

$$\gamma^s(N, N^m) = \frac{x^s}{\frac{1}{L}\left((N - N^m - 1)x^s + N^m x^m\right) + \sigma^2}, \tag{7.2}$$

where x^s and x^m are the symmetric power strategies for selfish and malicious users respectively.

The utility function of malicious user will be

$$U_i^m(\mathbf{x}) = \sum_{N^m=0}^{N} \mu^m(N, N^m)\left(U(\gamma_i^m(N, N^m)) + \theta_i \sum_{k\in S} U(\gamma_k^s(N, N^m))\right). \tag{7.3}$$

For the symmetric case,

$$\gamma^m(N, N^m) = \frac{x^m}{\frac{1}{L}\left((N - N^m)x^s + (N^m - 1)x^m\right) + \sigma^2} \tag{7.4}$$

is the SINR of malicious user.

Then the cost function of the malicious user for the symmetric case with $\theta_i = \theta^m,\ \forall\ i$ is

$$\begin{aligned} J^m(\mathbf{x}) = \alpha(C^m(\mathbf{x}) + B\frac{x^m}{h^m}) &- \sum_{N^m=0}^{N} \mu^m(N, N^m)(U(\gamma^m(N, N^m)) \\ &+ \theta^m(N - N_m)U(\gamma^s(N, N_m))). \end{aligned} \tag{7.5}$$

Next, as a special case we propose the model for the mechanism with two users and obtain the utility functions and cost functions. Let the probability belief of a regular user that another user is malicious be ψ^s and the probability belief of a malicious user that another user is regular be ψ^m. The total cost of regular user i including the price and energy cost will be,

$$J_i = \frac{Bx_i^s}{h_i} + \psi^s(C_i(x_i^s, x_j^m) - U_i\left(\gamma_i(x_i^s, x_j^m)\right)) + (1-\psi^s)(C_i(x_i^s, x_j^s) - U_i\left(\gamma_i(x_i^s, x_j^s)\right)) \quad (7.6)$$

The case when $\psi^s = 0$ will be the one with complete information. The cost function of malicious user i ,

$$\begin{aligned} J_i^m(x^s, x^m) &= \alpha_i B\frac{x_i^m}{h_i} + \psi^m(\alpha_i C_i(x_i^m, x_j^s) - U_i\left(\gamma_i(x_i^m, x_j^s)\right) \\ &- \theta_i U_j\left(\gamma_j(x_i^m, x_j^s)\right) + (1-\psi^m)\alpha_i C_i(x_i^m, x_j^m),\ j \neq i. \end{aligned} \quad (7.7)$$

We first analyze the complete information case for the comparison.

7.3 Pricing Mechanisms with Complete Information

With complete information and for the single carrier case, the optimal prices are given in equation (3.11) of Section 3.2.1. The prices with $n = 1$, in the N user case, modified with the energy cost $\mathbf{B}$, are obtained by the matrix equation,

$$A \cdot \mathbf{P} = D \cdot \mathbf{L} - \mathbf{B1}, \quad (7.8)$$

where

$$A := \begin{pmatrix} 1 & -\gamma_2 & \cdots & -\gamma_N \\ -\gamma_1 & 1 & \cdots & -\gamma_N \\ \vdots & & \ddots & \vdots \\ -\gamma_1 & -\gamma_2 & \cdots & 1 \end{pmatrix}, \quad D := \begin{pmatrix} \frac{1}{h_1} & 0 & \cdots & 0 & \frac{1}{h_1} \\ 0 & \frac{1}{h_2} & \cdots & 0 & \frac{1}{h_2} \\ \vdots & & \ddots & \vdots & \\ 0 & 0 & \cdots & \frac{1}{h_N} & \frac{1}{h_N} \end{pmatrix}, \quad (7.9)$$

For the two-users case, the price for User 1 turns out to be,

$$P_1 = \frac{1}{1-\gamma_1\gamma_2}\left(B\gamma_1\gamma_2 + \frac{\gamma_2(\lambda_1+\mu)}{h_1} + \frac{(\lambda_2+\mu)}{h_2}\right) \quad (7.10)$$

and similarly for User 2.

7.3.1 NE power allocation

Let us consider the case of linear SINR utility function $U_i(\gamma_i) = \gamma_i(\mathbf{x}),\ \forall i$.

Case 1: All users are regular

From the cost function given in equation (2.4), we obtain the KKT conditions for BR of user i as, $P_i + \frac{B}{h_i} - \frac{1}{\frac{1}{L}\sum_{j\neq i} x_j + \sigma^2} = 0$ and $x_i \geq 0, \forall i$. The powers of all the users at the NE is obtained as follows, by centrally solving this system of equations.

$$x_i = \frac{1}{N-1}\left[\sum_{j\neq i}\frac{L}{P_j + \frac{B}{h_j}} - (N-2)\left(\frac{L}{P_i + \frac{B}{h_i}}\right) - L\sigma^2\right]^+, \forall i. \tag{7.11}$$

Case 2: N^m users are malicious

The cost functions of all the N^m malicious users will be,

$$J_k^m = \alpha_k(P_k x_k^m + B\frac{x_k^m}{h_k}) - \gamma_k(\mathbf{x}) - \theta_k \sum_{j\neq k}\gamma_j(\mathbf{x}), \forall k. \tag{7.12}$$

The NE power can be only calculated numerically for the general case. Next we obtain the NE points analytically for the two-users case.

Proposition 7.1. *For the case, where $N = 2$ and $N^m = 1$, the NE power of User 2 who is malicious is*

$$x_2^m = \left[\frac{L}{P_1 + \frac{B}{h_1}} - L\sigma^2\right]^+, \tag{7.13}$$

and NE power of User 1 who is regular is

$$\theta_2 (x_1^s)^2 + x_1^s\left(\theta_2 L\sigma^2 - \alpha_2 L^2 \frac{\left(P_2 + \frac{B}{h_2}\right)}{\left(P_1 + \frac{B}{h_1}\right)^2}\right) - (1+\sigma^2)L^3\frac{\left(P_2 + \frac{B}{h_2}\right)}{\left(P_1 + \frac{B}{h_1}\right)^2} = 0. \tag{7.14}$$

Proof. The cost function of the malicious user is given by equation in (7.12), but for $N = 2$ and $N^m = 1$. The cost function of the regular user is same as (7.39). The powers of both the users at the NE is obtained by centrally solving the system of equations from the KKT conditions of BR. □

When the malicious user does not care about his self utility, the NE power of User 1 who is regular is

$$x_1^s = \frac{\alpha_2 L\left(P_2 + \frac{B}{h_2}\right)}{|\theta_2|\left(P_1 + \frac{B}{h_1}\right)^2}. \tag{7.15}$$

We could observe that when the User 2 is highly malicious, i.e. $|\theta_2|$ is high, the regular User 1 has less power. Apparently, both malicious and regular users takes less power when faced with higher price per unit power. Next, we obtain the PoM using the NE points obtained above.

Proposition 7.2. *For the two-users case with linear utilities for the case where the malicious user is interested in the self utility, PoM is given by,*

$$PoM(\mathscr{M}) := 1 - \left(\frac{\alpha_2 \left(P_2 + \frac{B}{h_2} \right)^2 (1 - \sigma^2 \left(P_1 + \frac{B}{h_1} \right))}{|\theta_2| \left(P_1 + \frac{B}{h_1} \right)^2 (1 - \sigma^2 \left(P_2 + \frac{B}{h_2} \right))} \right).$$

Proof. According to the Definition 2.21, for the two-users case,

$$PoM(\mathscr{M}) := \frac{\gamma_1(x_1, x_2) - \gamma_1(x_1^s, x_2^m)}{\gamma_1(x_1, x_2)},$$

where x_1 and x_2 are given by (7.11), x_1^s by (7.15) and x_2^m by (7.13). After the substitutions, we obtain the above result. □

Remark 7.1. We could observe that PoM increases when the user is highly malicious. For the symmetric case with $h_1 = h_2$ and $P_1 = P_2$, the windfall of malice occurs when $\alpha_2 > |\theta_2|$, i.e., when the malicious user cares more about the price and energy cost compared to the maliciousness effect. For $|\theta_2| = 1$, i.e., when the malicious user is extreme malicious, the windfall of malice never happens.

In the next section, we consider the Bayesian case with distributed pricing mechanisms.

7.4 Distributed Bayesian Pricing Mechanisms

In this section, we consider the Bayesian case where the users and designer have probabilistic information about others natures. We assume that if a user is regular, it receives the price P^s and if it is malicious P^m. We consider symmetric assumption where each user believes that other nodes of same type choose the same strategy.

7.4.1 BNE with an arbitrary number of malicious users

For an arbitrary number of malicious users with symmetry assumption, the cost function of a user, if it is regular, is given in equation (7.35) and if malicious, in equation (7.36). The BR of regular users is,

$$P^s + \frac{B}{h^s} - \sum_{N^m=0}^{N} \mu^s(N, N^m) \frac{LN^m x^m + L\sigma^2}{((N - N^m - 1)x^s + N^m x^m + L\sigma^2)^2} = 0.$$

The BR of malicious user is,

$$\alpha(P^m + \frac{B}{h^m}) - \sum_{N^m=0}^{N} \mu^m(N, N^m) L(\frac{(N-N^m)x^s + L\sigma^2}{((N-N^m)x^s + (N^m-1)x^m + L\sigma^2)^2} - \theta^m(N-N^m)\frac{Lx^s}{((N-N^m-1)x^s + N^m x^m + L\sigma^2)^2}) = 0.$$

The solution of the above two equations subject to $x^s \geq 0,\ x^m \geq 0$ gives the BNE with an arbitrary number of malicious users.

Proposition 7.3. *The BNE of the pricing game with an arbitrary number of malicious users with symmetric assumption is the solution of the below two equations subject to* $x^s \geq 0,\ x^m \geq 0$*;*

$$\sum_{N^m=0}^{N} \mu^s(N, N^m)(\gamma' + \frac{B}{h^s} - \frac{N^m h^m x^m + L\sigma^2}{\gamma^1\left((N-N^m-1)h^s x^s + N^m h^m x^m + L\sigma^2\right)^2}) = 0, \quad (7.16)$$

and

$$\sum_{N^m=0}^{N} \mu^m(N, N^m) L(\gamma'_\theta + \frac{B}{h^m} - \frac{(N-N^m)h^s x^s + L\sigma^2}{\gamma^1\left((N-N^m)h^s x^s + (N^m-1)h^m x^m + L\sigma^2\right)^2}) = 0, \quad (7.17)$$

$\gamma' = \dfrac{BN^m h^m x^m + L\sigma^2}{((N-N^m-1)h^s x^s + N^m h^m x^m + L\sigma^2)^2}$, $\gamma^{1m} = (1 + \gamma^m(N, N^m)))$ *and*
$\gamma'_\theta = \dfrac{(\alpha B + \theta^m)((N-N^m)h^s x^s + L\sigma^2)}{((N-N^m)h^s x^s + (N^m-1)h^m x^m + L\sigma^2)^2}$.

Proof. The BR of a regular user is obtained from the cost function in equation (7.35). Similarly, the BR of malicious users is obtained from the equation (7.36). From the definition of BNE in (3.38), we obtain the solution in the proposition. □

7.4.2 BNE for two-users case

The following proposition gives the BNE power strategies of the regular user and the malicious user with linear utilities.

Theorem 7.4. *For the two-users symmetric case, in the Bayesian pricing mechanism* $\mathscr{M}$*, the symmetric power strategy of the regular user at the BNE point for linear SINR utility functions is given by,*

$$x^s = \left[x^{s'}\right]^+, \quad (7.18)$$

and of the malicious user is the solution of

$$\alpha(P^m + Bh^m) - \frac{L^2|\theta^m|\psi^m x^{s'}}{(x^m + L\sigma^2)^2} - \frac{\psi^m L}{x^{s'} + L\sigma^2} = 0, \quad (7.19)$$

where

$$x^{s'} = \sqrt{\frac{L^2\sigma^2(1-\psi^s)}{P^s + \frac{B}{h^s} - \frac{\psi^s L}{x^m + L\sigma^2}}} - L\sigma^2. \tag{7.20}$$

Proof. For the two-users case, the cost function of a user, if it is regular, is given by equation (7.6) and if malicious, by equation (7.7). The BR from equation (7.6) gives the result in (7.20). From the KKT conditions of the BR using the other cost functions, we could obtain the BNE point. □

Without self utility for malicious user, from (7.19),

$$x^{s'} = \frac{(x^m + L\sigma^2)^2\alpha(P^m + \frac{B}{h^m})}{L^2|\theta^m|}. \tag{7.21}$$

We next compare the SINR obtained for the complete information case with x_1^s from equation (7.15) and x_2^m from equation (7.13) and the SINR for the Bayesian information case with x^s from equation (7.18) and x^m from equation (7.19). By this we obtain the boundary conditions under which the Bayesian case is better for the regular user. The conditions are not possible to obtain analytically but are numerically obtained in Numerical Section 7.9.

Proposition 7.5. *For the Bayesian pricing mechanism $\mathscr{M}$ with 2 users, one of the user is malicious and does not care about self utility and both the users have linear utilities, PoM is given by,*

$$PoM(\mathscr{M}) := 1 - \left(\frac{\alpha\psi^s \left(P^m + \frac{B}{h^m}\right)^2 (1 - \sigma^2\left(P^s + \frac{B}{h^s}\right))}{|\theta^m|(\left(P^s + \frac{B}{h^s}\right) - \frac{(1-\psi^s)L^2\sigma^2}{(x^s + L\sigma^2)^2}) \left(P^s + \frac{B}{h^s}\right)(1 - \sigma^2\left(P^m + \frac{B}{h^m}\right))} \right). \tag{7.22}$$

Proof. For this case,

$$PoM(\mathscr{M}) := \frac{\gamma_1(x_1, x_2) - \gamma_1(x^s, x^m)}{\gamma_1(x_1, x_2)},$$

where x_1 and x_2 are given by (7.11), x^s by (7.18) and x^m by (7.19). After the substitution we obtain the result in equation (7.22). □

Remark 7.2. We could observe that for this case also PoM increases when the user is highly malicious. PoM can be reduced by higher price for malicious user compared to the regular user, i.e, $P^m > P^s$. Windfall of malice happens when the second term on the right is greater than 1, i.e., $PoM < 0$. We could observe that when value of θ^m is close to 0 and ψ^s is close to 1, windfall of malice is possible. This is because the user is not malicious enough to have an effect and the user has higher expectation that the other

user is regular. At the same time, the regular user is aware that the other user can be malicious. The windfall of malice is also possible when the malicious user is charged very high compared to the regular user by the network and the user is highly price aware, i.e., with high α.

Next, we consider a special case where we look from the perspective of a regular user who tries to benefit from the uncertainty in the network. For this we analyze the case with User 1 who is inherently regular but it is of unknown nature to malicious User 2.

7.4.3 Two-users case: User 1 of unknown nature

We consider a malicious User 2 who faces User 1 of unknown nature and User 2 has only probabilistic information ψ^m about that user.

Proposition 7.6. *The power strategies of and the User 1 of unknown type at the Bayesian NE point for a game between two users of linear utility functions are given by,*

$$x_2^m = \left[\frac{L}{P_1 + \frac{B}{h_1}} - L\sigma^2 \right]^+, \tag{7.23}$$

x_1^s *given by solution of*

$$\psi^m \theta_2 (x_1^s)^2 + \left(\psi^m \theta_2 L \sigma^2 - \alpha_2 L^2 \frac{\left(P_2 + \frac{B}{h_2}\right)}{\left(P_1 + \frac{B}{h_1}\right)^2} \right) x_1^s - (1+\sigma^2)\psi^m L^3 \frac{\left(P_2 + \frac{B}{h_2}\right)}{\left(P_1 + \frac{B}{h_1}\right)^2} = 0 \tag{7.24}$$

and $x_1^m = 0$, where x_1^s and x_1^m are the powers of User 1 when it is regular and malicious user respectively, x_2^m be the received power at the base station for malicious User 2 and the prices P_1 and P_2 follow from (7.10).

Proof. The cost function of User 1 if it is regular is, $J_1^s = P^s x_1^s + B\frac{x_1^s}{h_1} - \gamma_2(x_1^s, x_2^m)$ and the cost function of User 1 if it is malicious is,$J_1^m = P^m x_1^m + B\frac{x_1^m}{h_1}$. User 2 has the utility function given in equation (7.7). The NE points can be obtained from the BRs. □

Remark 7.3. When the SINR of User 1 calculated from BNE in equations (7.23) and (7.24), is greater than the SINR it obtains from BNE in equations(7.13) and (7.14), the regular user benefits from the uncertainty it creates to the malicious user.

7.4.4 Pricing Mechanisms Resistant to Malicious Users

We consider the case where, the designer has only probabilistic information about malicious users and modifies the prices according to this information. Let $\mu^d(N, N^m)$ be the

joint probability mass function (pmf) of N and N^m as observed by the designer. Let us analyze how the designer can modify the pricing proposed in Section 7.3 using this information. The designer adds the utility of a user in the global objective only if that user is regular. Therefore, the designer maximizes the expected sum of utilities of selfish users according to the pmfs.

Theorem 7.7. *For the symmetric case, and $\mu^d(N, N^m) = \mu^s(N, N^m) = \mu^m(N, N^m)$, we obtain the optimal price for the regular users P^s as the same as in (7.8), but with modified matrix D^s given as,*

$$D^s := \frac{1}{h^s} \begin{pmatrix} \frac{1}{(N - \mathrm{E}[N^m])} & 0 & \cdots & 0 & 1 \\ 0 & \frac{1}{(N - \mathrm{E}[N^m])} & \cdots & 0 & 1 \\ \vdots & & \ddots & \vdots & \\ 0 & 0 & \cdots & \frac{1}{(N - \mathrm{E}[N^m])} & 1 \end{pmatrix}, \tag{7.25}$$

and the price for the malicious users P^m with the modified matrix D^m given as,

$$D^m := \frac{(1 - \theta^m \gamma^s)}{h^s} \begin{pmatrix} \frac{1}{(N - \mathrm{E}[N^m])} & 0 & \cdots & 0 & 1 \\ 0 & \frac{1}{(N - \mathrm{E}[N^m])} & \cdots & 0 & 1 \\ \vdots & & \ddots & \vdots & \\ 0 & 0 & \cdots & \frac{1}{(N - \mathrm{E}[N^m])} & 1 \end{pmatrix},$$

where $\mathrm{E}[N^m] = \sum_{N^m=0}^{N} N^m \mu^d(N, N^m)$.

Proof. For the symmetric case, when all users are of unknown type with arbitrary number of malicious users, the global objective of the designer in (7.41) changes as,

$$\max_{x^s, x^m} \sum_{N^m=0}^{N} (N - N^m) \mu^d(N, N^m) U(\gamma^s(N, N^m)) \tag{7.26}$$

s. t. $\sum_{N^m=0}^{N} (N - N^m) \mu^d(N, N^m) x^s \leq X_{max},\ x^s \geq 0\, x^m \geq 0$
where $\gamma^s(N, N^m)$ is given by (7.36). The prices are obtained as the same way of alignment of user and designer objective through prices as in [39] with the modified designer objective. □

We could observe that the users receive higher prices when there is a higher expectation of number of malicious users in the network. Also, the price for the malicious users are higher with higher degree of maliciousness.

7.5 Centralized Bayesian Auctions with Malicious Users

Now we consider auction mechanisms in which the designer (base station) makes centralized decisions on the power level and price for all users. This is the case in the practical wireless networks and standards now, like OFDMA with centrally controlled resource coordination in 3GPP- LTE system [106]. We analyze, how the uncertainty about the type of users, affect the user strategies in the auction mechanisms proposed in Section 6.2.4 of Chapter 6.

Consider the two-users symmetric case with both the users of uncertain type and log utility for all the users. The cost function of the regular User i anticipating that it will receive an SINR given in (7.31) is

$$\begin{aligned} J_i &= \psi^s(B\frac{x_i^s}{h_i(x_i^s+x_j^m)}Q_{max} + x_i^s x_j^m - \log(\frac{x_i^s Q_{max}L}{x_j^m(Q_{max}+\sigma^2 L)+x_i^s\sigma^2 L})) \quad (7.27)\\ &+ (1-\psi^s)(B\frac{x_i^s}{h_i(x_i+x_j^s)}Q_{max} + x_i^s x_j^s - \log\left(\frac{x_i^s Q_{max}L}{x_j^s(Q_{max}+\sigma^2 L)+x_i^s\sigma^2 L}\right)) \end{aligned}$$

where x_j^s and x_j^m are the strategies of User j when it is regular and bot respectively. User i minimizes J_i subject to $x_i^s \geq 0$. The cost function of User i if it is malicious is,

$$\begin{aligned} J_i^m &= \psi^m(x_j^s x_i^m + B\frac{x_i^m}{h_i(x_j^s+x_i^m)} - \log\left(\frac{x_i^m Q_{max}L}{x_j^s(Q_{max}+\sigma^2 L)+x_i^m\sigma^2 L}\right) \quad (7.28)\\ &- \theta_i \log\left(\frac{x_j^s Q_{max}L}{x_i^m(Q_{max}+\sigma^2 L)+x_j^s\sigma^2 L}\right)) + (1-\psi^m)(B\frac{x_i^m}{h_i(x_j^m+x_j^s)}Q_{max} + x_i^m x_j^m). \end{aligned}$$

The strategies of the users can be obtained by solving the system of equations obtained from the best responses. Since they are not analytically tractable, the numerical simulation is given in Section 7.9.

7.5.1 Auction Mechanism Resistant to Malicious Users

In this section, we modify the pricing rule in the auction mechanism given in the previous section, according to the individual probabilities of users being malicious ones. Let ψ_j^d is the probability of user j being malicious, which is constructed by the designer from the detections given in the Section 7.8. The users will be discouraged from acting malicious, when faced with pricing from the designer, using ψ_j^d, $\forall\ j$ and θ_j, $\forall\ j$. The same problem for the complete information case is analyzed and a *differentiated pricing* for malicious users is proposed in Proposition 6.19in Section 6.5. The auction mechanism resistant to malicious users using Bayesian information is given next.

Proposition 7.8. *For a wireless network with users having logarithmic utilities, the auction mechanism with the allocation*

$$Q_j(\boldsymbol{x}) = \frac{x_j}{\sum_k x_k + \omega}\, Q_{max},\ \forall\ j. \quad (7.29)$$

and the pricing

$$\begin{aligned} C_j(\boldsymbol{x}) &= x_j \sum_{k \neq j} x_k + \omega \\ &- \psi_j^d (N-1)\theta_j t Q_{max} \log\left(1 + \frac{x_j}{\sum_{k \neq j} x_k}\right) \end{aligned} \tag{7.30}$$

will force the users to act as regular users in the network, where $t = \sum_k x_k$.

Remark: The proof of the proposition is similar to the proof of Proposition in Section 6.5. The allocation in equation (7.29) makes sure the full utilization of the powers when $\omega = 0$, i.e.

$$\sum_j Q_j = Q_{max}.$$

Using the full utilization property of the proportional allocation,the SINR of a user can be made function of allocation of only that user,

$$\gamma_i(Q_i(\mathbf{x})) = \frac{Q_i(\mathbf{x})}{C - Q_i(\mathbf{x}) + \sigma^2}. \tag{7.31}$$

To obtain the pricing rule, an additional pricing term is added to the prices in equation (6.11), proportional to the degree of maliciousness of the users. To obtain the pricing rule for the Bayesian case as in equation (7.30), we follow the same steps in the proof of Proposition 6.19 in Section 6.5.

7.6 Bayesian Mechanisms for Security of Wireless Network with QoS Requirements

In this section, we analyze pricing to satisfy the QoS requirements at the equilibrium point of the game in the previous section. Each user reports a QoS (rate) requirement $\underline{u}_i$ to the base station. In this section, the Shannon rates are considered as the utility functions in this section, i.e.,

$$U_i(x_i, x_{-i}) = \log\left(1 + \gamma_i(\mathbf{x})\right) \quad \forall i \in \mathscr{A}. \tag{7.32}$$

and every user receives a price μ_i per SINR. The QoS requirements are satisfied if

$$U_i(x_i, x_{-i}) \geq \underline{u}_i, \quad \forall i \in \mathscr{A}. \tag{7.33}$$

where $\underline{u}_i$ is the QoS (rate) requirement of user i.

The power allocation to achieve the QoS requirement $\underline{u}_i$ of each user is proved in [104] as

$$x_i^U = \frac{B_N}{h_i} \cdot \frac{2^{\underline{u}_i} - 1}{2^{\underline{u}_i}}, \ \forall\ i,$$

where $B_N = \frac{1}{\sum_{j=1}^{N} \frac{1}{2^{\underline{u}_j}} - N + 1}$ is a constant for given $\underline{u}_j, j = 1, \cdots, N$.

The individual optimal prices which make the NE $\mathbf{x}^{NE}$ equal to $\mathbf{x}^U$ are obtained in [105] as

$$\mu_i = \frac{h_i}{2^{\underline{u}_i}},\ \forall\ i. \tag{7.34}$$

The cost function of the regular user with SINR pricing will be,

$$J_i^s(x^s, x^m) = \sum_{N^m=0}^{N} \mu^s(N, N^m)(\mu_i \gamma_i^s(N, N^m) + B\frac{x_i^s}{h_i} - U(\gamma_i^s(N, N^m)). \tag{7.35}$$

For the symmetric case, when the channel gains of all the regular users and malicious users are equal to h^s and h^m respectively, the SINR of regular users become

$$\gamma^s(N, N^m) = \frac{h^s x^s}{\frac{1}{L}\left((N - N^m - 1)h^s x^s + N^m h^m x^m\right) + \sigma^2}$$

where x^s and x^m are the symmetric power strategies for selfish and malicious users respectively.

The utility function of malicious user is

$$U_i^m(\mathbf{x}) = \sum_{N^m=0}^{N} \mu^m(N, N^m)\left(U(\gamma_i^m) + \theta_i \gamma_i^m\right).$$

For the symmetric case,

$$\gamma^m(N, N^m) = \frac{h^m x^m}{\frac{1}{L}\left((N - N^m)h^s x^s + (N^m - 1)h^m x^m\right) + \sigma^2}$$

is the SINR of malicious user.

Then the cost function of the malicious user for the symmetric case with $\theta_i = \theta^m,\ \forall\ i$ is

$$J^m(\mathbf{x}) = \sum_{N^m=0}^{N} \mu^m(N, N^m)(\alpha(\mu\gamma^m(N, N^m) + B\frac{x^m}{h^m}) - U(\gamma^m(N, N^m)) + \theta^m \gamma^m(N, N_m)).$$

First we discuss the pricing with complete information and extend it to Bayesian case later.

7.6.1 Differentiated Pricing with Complete Information

The price and NE power allocation, with QoS requirement and complete information about the type of users and identities, are obtained in [105]. With the individual price $\mu_i = \frac{\alpha_i}{2^{\underline{u}_i}},\ \forall\ i$, the Nash equilibrium power allocation $x_i^{NE}(\theta_i)$ of each user i in the

noncooperative game $\mathscr{G}$ in the general MAC system with private type θ_i is higher than or equal to x_i^U in (7.34), where

$$\underline{x}_i^{NE}(\theta_i, \theta_{-i}) = \frac{1 - \theta_i - 2^{-\underline{u}_i}}{\alpha_i \sum_{j=1}^{N}(2^{-\underline{u}_j} + \theta_j) - N + 1}, \ \forall \ i. \tag{7.36}$$

The resulting rate $U_i(\theta_i)$ is

- $U_i(\theta_i) = \underline{u}_i$, for selfish users with $\theta_i = 0$
- $U_i(\theta_i) > \underline{u}_i$, for malicious users with $0 < \theta_i \leq 1$.

If all the users are selfish, the NE power allocation will be as in equation (7.36) but with $\theta_i = 0, \ \forall \ i$.

In differentiated pricing, the malicious user is punished with price μ^m and the selfish user by μ^s. In the N-user non-cooperative game $\mathscr{G}$ of general MAC system, no malicious user will have incentive to behave maliciously if the punishment price [105] μ_i^m is given by

$$\mu_i^m \geq \mu_i^s - \theta_i h_i, \ \forall \ i. \tag{7.37}$$

To implement the pricing the designer need to know the exact identity of the malicious user here. But this is not realistic. Therefore, we propose a Bayesian differentiated pricing in the next section.

7.6.2 Bayesian Pricing with QoS Requirements

We assume that to implement Bayesian differentiated pricing, the designer observes each user in the network and attach a probability that he is malicious [21]. Let ψ_i^d be the probability that user i is malicious and θ_i^d be the estimate of degree of maliciousness of user i by the designer. Since it is not realistic to estimate the exact value of the degree of maliciousness θ_i by the designer, we assume that he gives the maximum punishment, i.e., with $\theta_i^d = -1$. Each user's Bayesian price according to the probabilities are;

$$\mu_i^m = \frac{h_i}{2^{\underline{u}_i}} - \psi_i^d \theta_i^d h_i. \tag{7.38}$$

We consider also that there may be an error in the estimation of probability by the designer. With the Bayesian pricing, for the two-users case, the cost of the regular user becomes

$$\begin{aligned} J_i &= B\frac{x_i^s}{h_i} + \psi^s((\mu_i^s - \psi_i^d\theta_i^d h_i)\gamma_i^{sm}) \\ &- U_i\left(\gamma_i^{sm}\right)) + (1 - \psi^s)((\mu_i^s - \psi_i^d\theta_i^d h_i)\gamma_i(x_i^s, x_j^s) - U_i\left(\gamma_i(x_i^s, x_j^s)\right)), \end{aligned} \tag{7.39}$$

and for malicious user

$$\begin{aligned} J_i^m &= \alpha_i B\frac{x_i^m}{h_i} + \psi^m(\alpha_i(\frac{h_i}{2^{\underline{u}_i}} - \psi_i^d\theta_i^d h_i)\gamma_i(x_i^m, x_j^s) \\ &- U_i(x_i^m, x_j^s) - \theta_i\gamma_i(x_i^m, x_j^s)) + (1 - \psi^m)\alpha_i(\frac{h_i}{2^{\underline{u}_i}} - \psi_i^d\theta_i^d h_i)\gamma_i(x_i^m, x_j^m), \end{aligned} \tag{7.40}$$

where $\gamma_i^{sm} = \gamma_i(x_i^s, x_j^m)$. The BNE can be obtained from these cost functions.

In the Section 7.8.3, we propose a way of detecting the malicious users observing the anomalies in the utility function. For this purpose, the designer learns the utility functions of all the users from their BR strategies.

In the numerical section, we calculate the BNE numerically with the prices given in equation (7.38). Then we compare the Bayesian case, to the complete information case.

7.7 Truthful Bayesian Mechanism

Next, we study mechanisms in which the users report their type (θ which indicates if it is regular or malicious) to the network designer in addition to bidding on its power. Every user does two thing, reports its type (θ value) and responds to the power allocation and pricing rule from the designer with a scalar bid. The designer asks the users to bid their type and wants to make the users bid their true type. The designer additionally has probability distribution of the types of users. We analyze mechanism for truthful implementation in a Bayesian environment, which forces regular and malicious users to report their true nature using the reported types, scalar bids and the probability distribution of user types.

There is an efficient, budget balanced (sum of the payment is zero) and truthfully implementable mechanism in Bayesian Nash equilibrium if the prices follow the classical d'Aspremont Gerard-Varet Arrow (dAGVA) [41] pricing scheme. A truthfully implementable mechanism in Bayesian Nash equilibrium for wireless ad-hoc networks was proposed in [91], without taking interference into account. We extend the dAGVA mechanism to counter malicious users in an interference limited wireless network.

Proposition 7.9. *For the truthful mechanism in the presence of malicious users, the allocation is*

$$Q^*(\boldsymbol{x}, \theta) = \max_{\boldsymbol{Q}} \sum_i U_i(\gamma_i(\boldsymbol{Q(x)}), \theta_i),\ Q_i(\boldsymbol{x}) \ \geq\ 0\ \forall\ i, \tag{7.41}$$

Q^* is the efficient allocation which maximizes the sum of expected user utilities and the pricing is given by,

$$C_i(\boldsymbol{x}, \theta) = -E_{\theta_{-i}}\left[\sum_{k\neq i} U_k^m(\gamma_k(Q_k^*(\boldsymbol{x}), \boldsymbol{Q}_{-k}^*), \theta_k)\right] - M_i(\boldsymbol{x}, \theta_{-i}) \tag{7.42}$$

where $M_i(.)$ is any function of θ_{-i} and the calculations are done using the reported types. For the budget balance mechanism (which does not need external supply of money to the designer), $M_i(.)$ is taken as,

$$M_i(\boldsymbol{x}, \theta_{-i}) = \frac{-1}{(n-1)} \sum_{j\neq i} E_{\theta_{-j}}\left[\sum_{k\neq j} U_k^m(\gamma_k(Q_k^*(\boldsymbol{x}), \boldsymbol{Q}_{-k}^*), \theta_k)\right] \tag{7.43}$$

Here the total price $C_i(\mathbf{x}, \theta)$ is the difference in sum of utilities of other users with and without the presence of user i. The designer asks the users to report their θ values which indicate their level of maliciousness. The above allocation and pricing makes them report the true values if they are regular which can be proved in the line of proof in [41]. When the malicious user reports true θ value, he will be forced by the mechanism to pay a higher price. Then the malicious user can choose to stay in the system paying the price until he is removed from the network. Otherwise, the malicious user could report that he is regular or report as a malicious user with less maliciousness. But in the case of false reporting, the malicious user will have higher cost due to the allocation and pricing of the truthful mechanism in Proposition 7.9. Therefore, if the malicious user bear the higher individual cost, he can hide as a regular user or a malicious user with small maliciousness capability. In the simulation section, we quantify the additional price paid by the malicious user as a function of degree of maliciousness θ.

7.8 Malicious User Detection

We study the detection of botnets [49] observing the resource allocation and *virtual* prices in the mechanism. The detection using the mechanism itself gives the network operator a chance to avoid the burden of an additional detection scheme. The observation of the network mechanism is performed over a long period of time by the network. The resource usage when there are automatic queries (calls, texts, data traffic) by the bot creates a pattern. The *virtual* prices in the pricing mechanism also reflect the use of resources by the bots. The operator can detect bots observing these prices and after the detection can inform the mobiles that they are being compromised. Detection and prevention of the bots in the BS itself will reduce the possibilities of the congestion and DoS at the network core.

7.8.1 Bayesian hypothesis testing

We perform hypothesis testing in this section. Let the hypothesis that a mobile is bot or not are H1 and H0 respectively. Let the payment by the user i in the slot t is $C_{it} = P_{it}x_{it} \in R$ and the allocation is $x_{it} \in R$ in the pricing mechanism. The rule for testing, observing the allocation in one time instant, is given as follows:

$$\gamma_0 = 1, \text{ if } \frac{p_1}{p_0} \geq \frac{\pi_0}{\pi_1};\ \gamma_0 = 0, \text{ otherwise,}$$

where $p_1 = p(X_i = x_{it}|H_1)$ and $p_0 = p(X_i = x_{it}|H_0)$ and π_0 and π_1 are prior probabilities of H_0 and H_1 respectively.

Now we use the time correlation of data for the test. We observe the allocation, pricing and channel gains over T number of time slots and use them as the features of the training set. The allocation and pricing are connected to the average and the standard deviation of a number of sent/received packets. When a mobile is bot, the data traffic is higher with a certain pattern. Therefore, we form an auto-correlation of the training vector.

$$r_i = \frac{\sum_{t=1}^{T-1}(x_{it} - \bar{x})(x_{it+1} - \bar{x})}{\sum_{t=1}^{T}(x_{it} - \bar{x})}$$

The rule for the testing using the auto-correlation is given as follows: $\gamma_0 = 1$, if $\frac{p_1}{p_0} \geq \frac{\pi_0}{\pi_1}$; $\gamma_0 = 0$, otherwise, where $p_1 = p(R_i = r_i|H_1)$ and $p_0 = p(R_i = r_i|H_0)$.

Next we propose a more decentralized approach in which some regular users also act as detectors, in addition to the BS (designer). In this detection approach, N^s regular users do hypothesis testing to see if another user is a regular or a bot and send the results to the designer. $\gamma_0 = 1$, if $\frac{p_1(l_1, \cdots, l_N^s)}{p_0(l_1, \cdots, l_N^s)} \geq \frac{\pi_0}{\pi_1}$; $\gamma_0 = 0$, otherwise, where p_1 and p_0 are conditional probability mass functions given H_0 and H_1 respectively.

7.8.2 Detection using machine learning

Detections using different machine learning classifiers [85] are discussed in this section. To form the training vector, we could obtain traffic of users using our model or using real data of bot and regular traffic. Using the training set, we perform the classification of the test data into two classes; bot and regular. We consider here, pricing mechanisms explained in Section 7.4. We first obtain channel gain, allocation and pricing over T number of time slots using our model in Section 7.2 randomly. For a specific set of channel gains, the allocation and pricing of regular user in slot t is given by equations (7.13) and (7.14) respectively. Below is the list of classifiers we consider in this section.

1. **Support Vector Machine (SVM)**: SVM is a good classifier to utilize the time correlation in test data. In the numerical section, we plot the support vectors obtained from the SVM method.

2. **Naive Bayes:** In this probabilistic classifier, the assumption is that the features are conditionally independent.

3. **K-Nearest Neighbor(KNN):** It is a nonparametric classifier known for its simplicity. A shortcoming of the KNN algorithm is that it is sensitive to the local structure of the data.

In the numerical section, we compare the different classifiers.

7.8.3 Detection by learning the anomalies in the utility functions

The designer needs to know the utility functions to find the prices in the previous sections. In addition, the designer needs to know the identities of the malicious user to implement the pricing. In this section, regression techniques are used to learn the user utilities by the designer. Here, the anomalies in the marginal utility curves are used to obtain the identities of malicious users. The information about the identities of malicious users with a possible error is used in the model in Section further for implementation of

the differentiated pricing mechanism. The detection uses the fact that the prices in the pricing mechanism also reflect the use of resources by the malicious users. The utility function of a user is not assumed to be Shannon rate in this section and it can be any concave function of the SINR.

The regular user optimization problem will be to find the power level which minimizes the regular individual cost , i.e.,

$$\min_{x_i} \quad P_i x_i + B\frac{x_i}{h_i} - U_i\left(\gamma_i(\mathbf{x}_{-i}, x_i)\right),$$

Consequently, the general condition for player best response obtained from first order derivative is

$$P_i + \frac{B}{h_i} - \frac{dU_i(x)}{d\gamma_i}\frac{1}{I_i(\mathbf{x}_{-i})} = 0, \ \forall \ i \in \mathscr{A}. \tag{7.44}$$

First, the designer gives sample values of prices $\mathbf{P}$ to all the users. Then the designer observes the NE $\mathbf{x}^{NE}$ and calculates the interference at the NE, $\mathbf{I}^{NE}$ of all the users. At the NE,

$$P_i = U_i'\frac{1}{I_i^{NE}} - \frac{B}{h_i}, \ \forall \ i \in \mathscr{A}, \tag{7.45}$$

where $U_i' = \dfrac{dU_i}{d\gamma_i}$, $\forall \ i$. With different values of $\mathbf{P}$, the designer can plot the curve of U_i' against γ_i using a method like regression leaning given in [32].

For the malicious user,

$$P_i = U_i'\frac{1}{I_i^{NE}} - \frac{B}{h_i} - \theta_i \sum_{k\in S}\frac{dU_k(\gamma_k)}{d\gamma_i}, \ \forall \ i. \tag{7.46}$$

The designer will obtain a completely different type of curve U_i' for the malicious users. The designer uses this anomaly in the curve for the detection of malicious users and punish them with higher price.

The detection and pricing is part of the mechanism and can be implemented online. The learning process requires first a training phase where the users are given sample prices and then their actions are observed. The exchange of prices and actions, which are real numbers, can be done over the control channel with communication overhead which is a function of the number of training slots. Then the marginal utility functions can be updated online just by observing the user actions which are already available with the designer. The computational overhead involves fitting the function using a method like regression leaning given in [32]. In addition to the pricing and providing channel information feedback to different users, the base station has a network security module which detects the malicious users and update the probability beliefs. The designer can first build the pmf by giving sample prices and observing the best responses for detection. Then the pmfs can be updated in an online fashion every time slot or in every several time slots. The detections facilitate the designer to update the probability beliefs with the changing parameters in the wireless network.

7.9 Numerical Results

Now, we numerically evaluate the results which were obtained in the previous sections.

7.9.1 Simulations for Bayesian mechanisms

First, we obtain the NE powers of regular and malicious user in pricing mechanism with Bayesian information which is proposed in Section 7.4. We consider arbitrary number of malicious users out of $N = 50$ users. We take the symmetric assumption given in Section 7.4. The distributions $\mu^s(N, N^m)$ and $\mu^m(N, N^m)$ are taken as binomial distribution. The NE powers are plotted as a function of probability p in binomial distribution in Figure 7.1. The wireless parameters are $\sigma = 0.1$ and $L = 0.01$. The malicious user parameters are $\theta = -0.5$ and $\alpha = 0.8$. It is observed that when $p = 0.8$ the malicious users have the highest impact on the power of regular users. Next, we simulate auction mechanisms given in Section 7.5 with $N = 20$ users out of which only one user j is of uncertain type and others are regular users. We take symmetric assumption with all regular users have same channel gains. The NE points are obtained by solving the BR obtained from the cost functions given in equations (7.27), (7.28). The system parameters used are $\psi^m = \psi^s = 0.5, \omega = 0$ and $X_t = 1$. In Figure 7.2, the NE points are plotted for complete information and Bayesian case as a function of θ_j. For the complete information case, the user j is a malicious user and others are regular. We could see that when $\theta_j > -0.42$, the user j benefits from the uncertainty. The User j benefit from the uncertainty when it is less malicious, i.e., when θ_j is close to 0.

Next for the truthful Bayesian mechanism given in Proposition 7.9, the difference in prices for 19 regular users and a malicious user is obtained. The prices are plotted as a function of the degree of maliciousness of the malicious user in Figure 7.4. In Figure 7.3, we plot the additional cost the malicious user needs to incur if he does false reporting as a regular user ($\theta = 0$). We could observe that when the malicious user is originally more malicious he receives higher cost for hiding as a regular user.

7.9.2 Simulations for Malicious User Detection

First, for the hypothesis testing, we obtain the conditional distribution of rate allocations in the auction which was presented in Section 7.5 in Figure 7.5. The channel gains are obtained as uniform random numbers. Other system parameters remain the same as in the previous subsection. These conditional distributions form the basis for the hypothesis testing given in Section 7.8.1.

Next, the plot of the SVM model is given in Figure 7.6. It is obtained using the training data produced with the system model for the auction given in Section 7.5. Using this SVM model, classification of the users can be done into bots and regular users. Now we compare different machine learning schemes for detecting bots and the results are given in Table 7.1. To evaluate each classifier, the 70-percent split validation method is used. The results are expressed in terms of the following performance measurements. For each classifier, true positive rate (TPR), which is the probability of correctly detecting

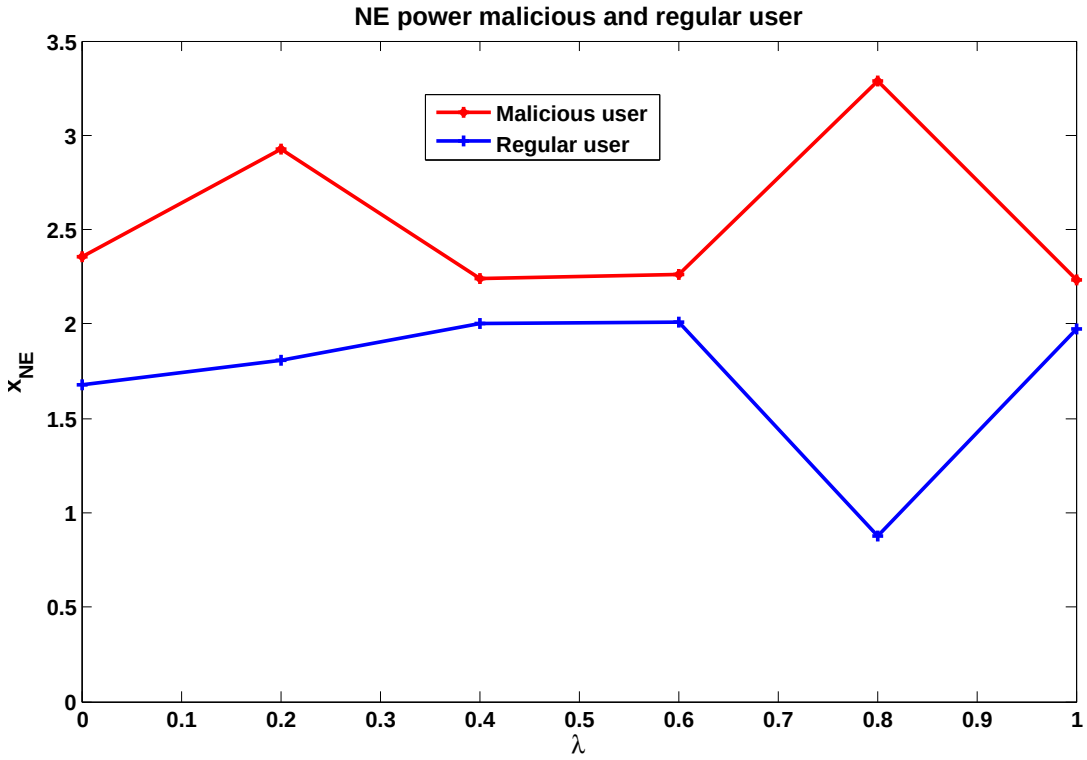

Figure 7.1: The variation of NE points in pricing mechanism with Bayesian information in Section 7.4, for an arbitrary number of malicious users, as a function of probability λ in the binomial distribution.

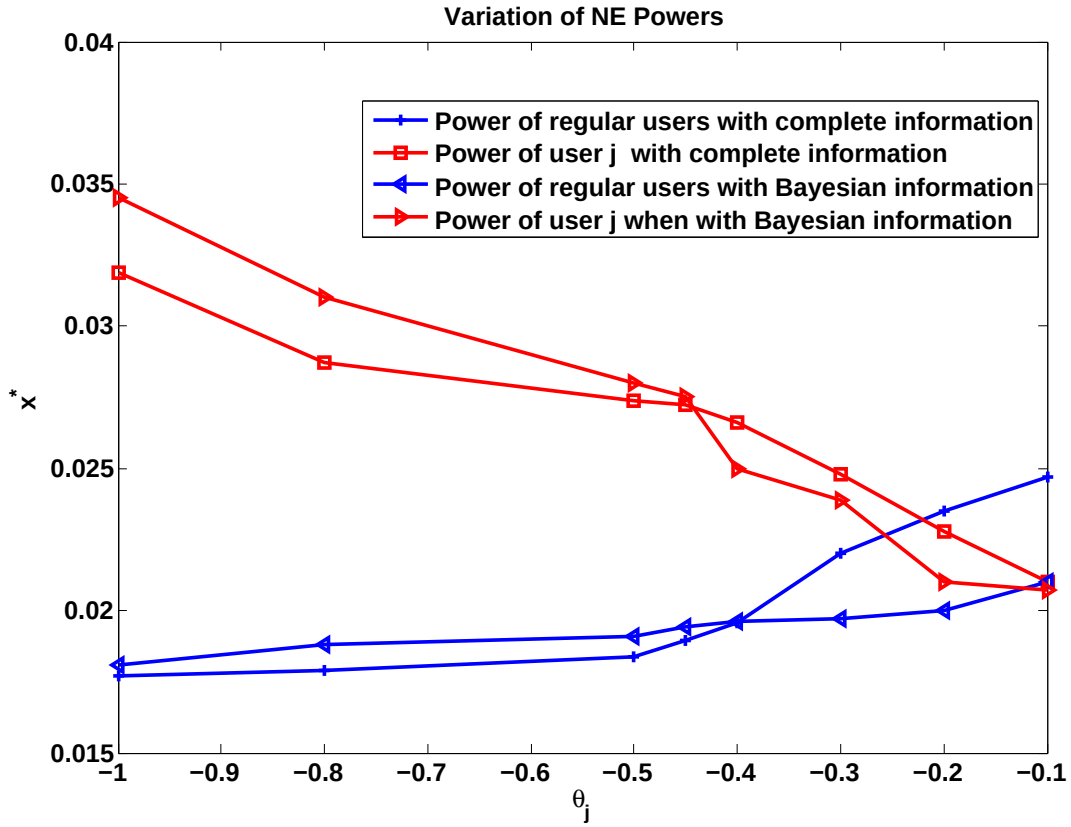

Figure 7.2: The variation of NE points with and without complete information in auction, as a function of degree of maliciousness θ_j.

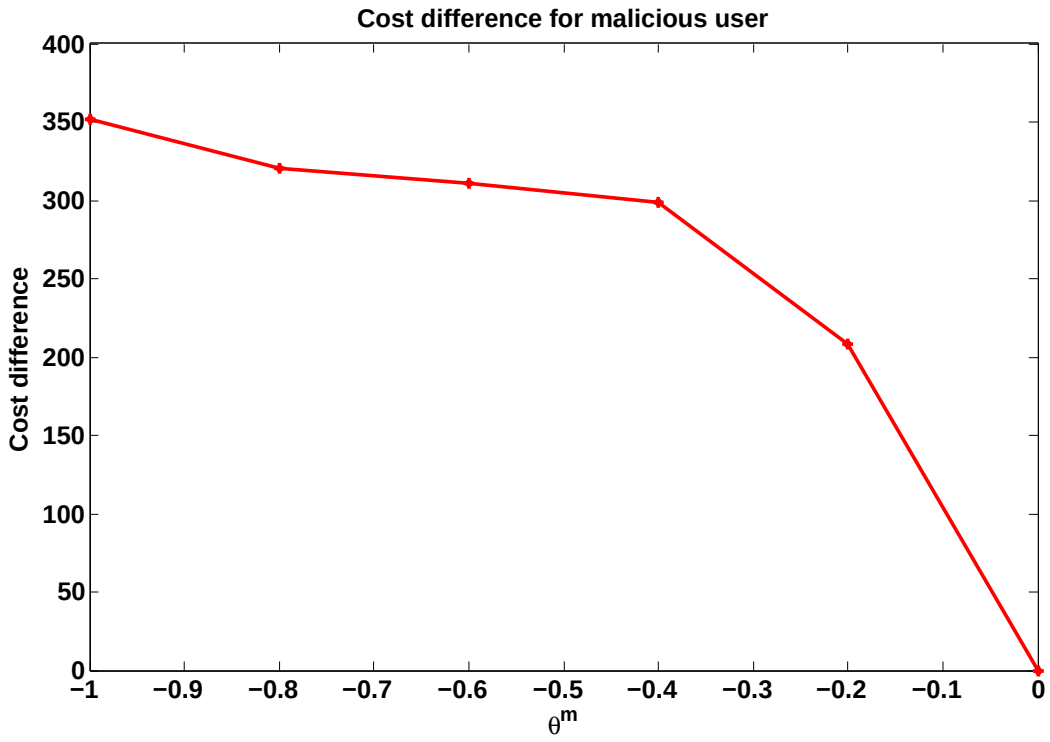

Figure 7.3: The plot of additional cost for the malicious user when he reports $\theta = 0$, as a function of his true degree of maliciousness, in truthful Bayesian mechanism.

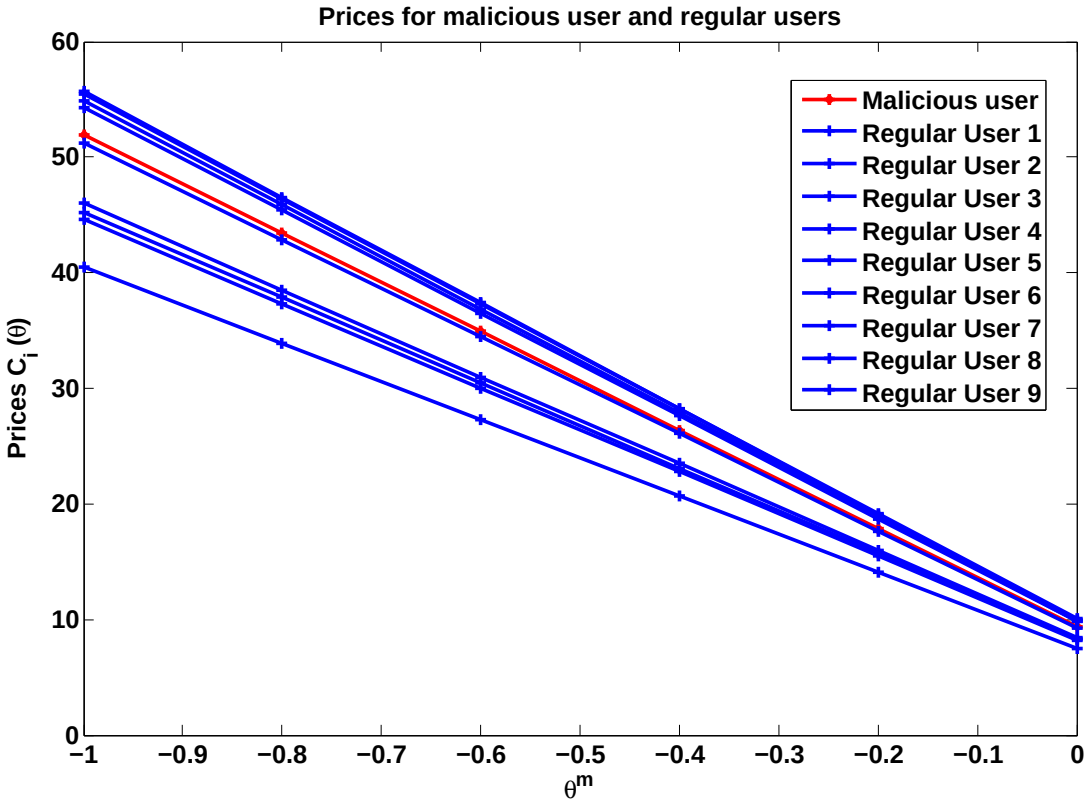

Figure 7.4: The variation of prices as a function of the degree of maliciousness in truthful Bayesian mechanism.

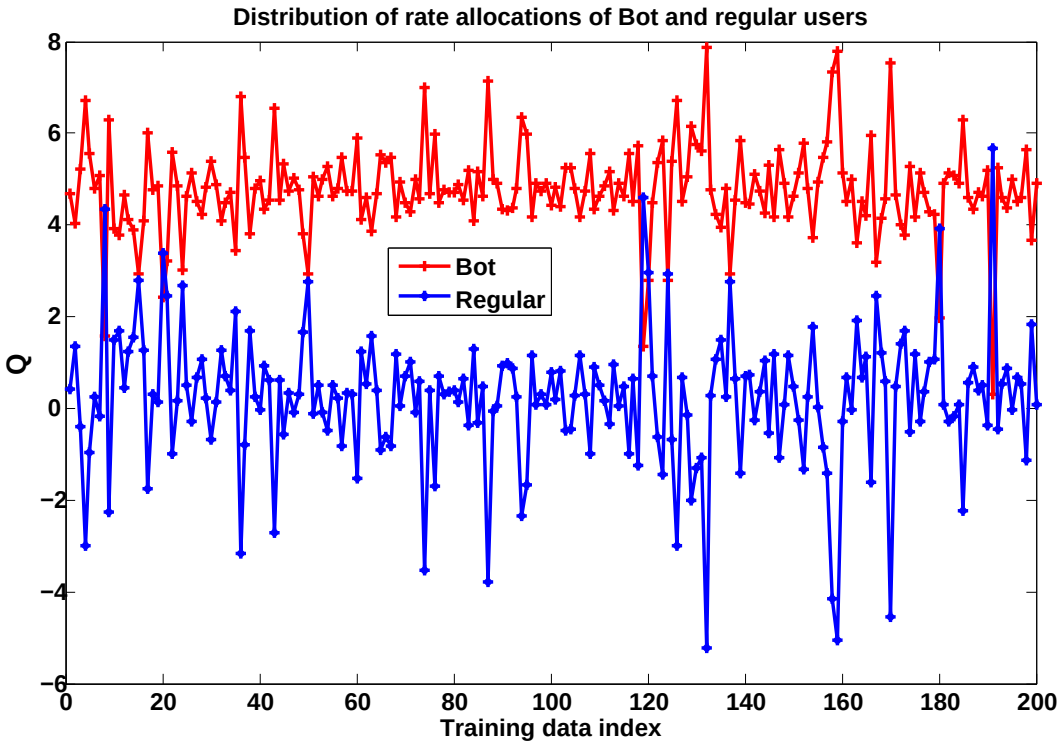

Figure 7.5: The conditional distributions of rate allocations and the prices for bot and regular user.

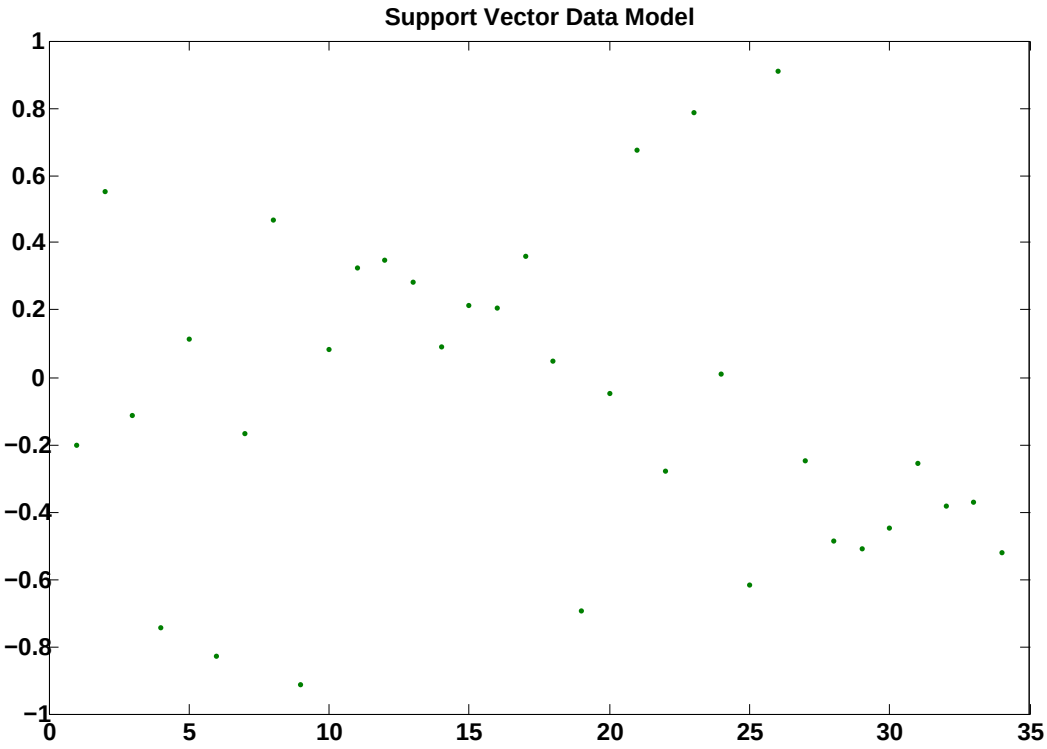

Figure 7.6: The support vectors obtained from the training data of allocation for bot and regular user.

a mobile as bot, is calculated. Additionally, false positive rate (FPR) which is another measurement defined as the false detection of regular mobile as bot, is also listed in Table 7.1. We could observe that KNN method has the lowest TPR and highest FPR among the three methods. Also SVM has lower FPR and TPR compared to Naive Bayes.

Classifier	TPR	FPR
SVM	0.9871	0.063
Naive Bayes	0.98731	0.0729
KNN	0.9713	0.1629

Table 7.1: Detection performance of different machine learning schemes

7.9.3 Numerical analysis with real botnet data

Here, we use a real dataset, which is capture of bot and normal traffic in [47], as the basis for the simulations. We add wireless model with interference to the regular and bot IP addresses over this real dataset from wired IP addresses. We consider the pricing mechanisms proposed in Section 7.4 for the simulation. Depending on the traffic, the prices are obtained from the equation in equation (3.11) of Section 3.2.1. The file we use here has the netflows generated by an unidirectional Argus. The dataset included the date and time of capture, flow duration, protocol of transmission, source IP address, destination IP address, flags, Type of Service (ToS), number of packet bytes and the labels. The labels were assigned as follows:

1. Background; for the traffic from all the computers in the university.

2. Legitimate; for the traffic that matches some IP addresses which are checked prior and made sure not infected. In the dataset there are 21 different legitimate IP addresses.

3. Botnet; for the traffic that comes to or from the IP address 147.32.84.165.

The packet byte data is used as the amount of traffic from different IP addresses and channel gains are added to them. Interference and prices are calculated as in Section 7.4. We first train the detectors using the data from the Legitimate computers and botnet. Then the data from different IP addresses, which are labeled background, are tested to detect bots.

The conditional distributions of number of bytes from one of the Legitimate IP address and bot IP address are plotted in Figure 7.7. Next, anomaly detection using the data from Background data in [47] is carried out. In Figure 7.8, the result of the detection of bot from the IP addresses in Background data, using KNN search method, is plotted. The labels are given as -1 for Bot and 1 for regular IP addresses respectively for 50 IP addresses.

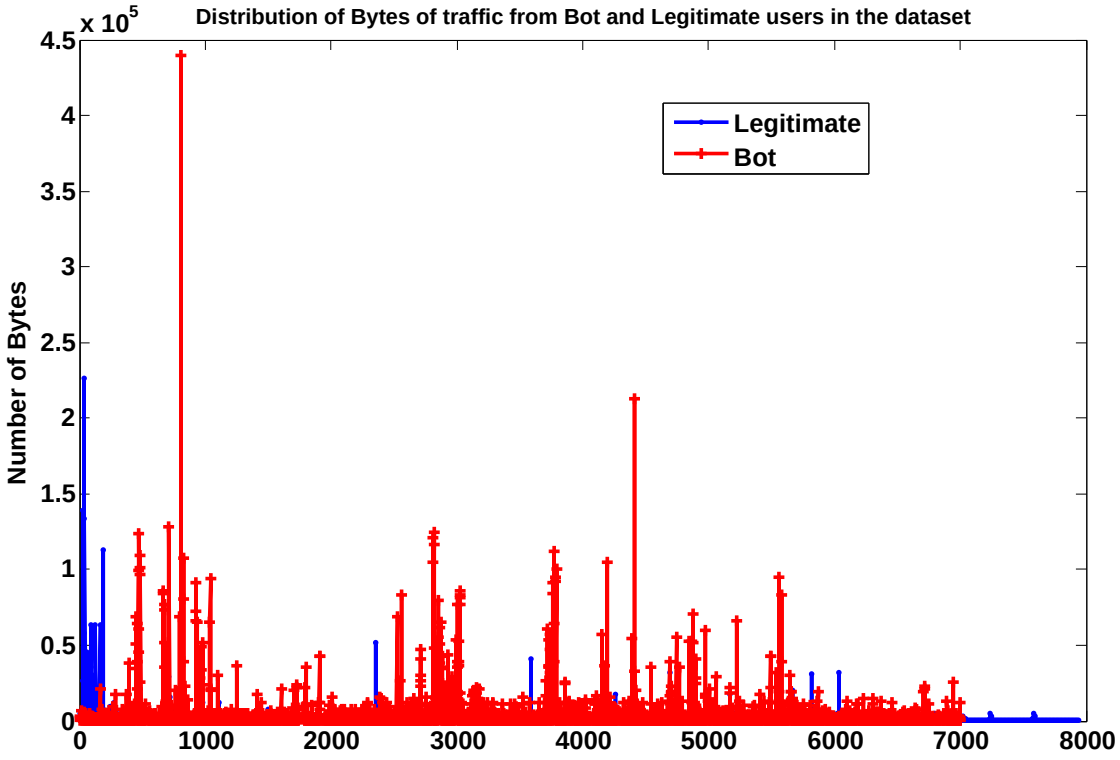

Figure 7.7: The distributions of number of packet bytes used by the bot and regular user in the dataset.

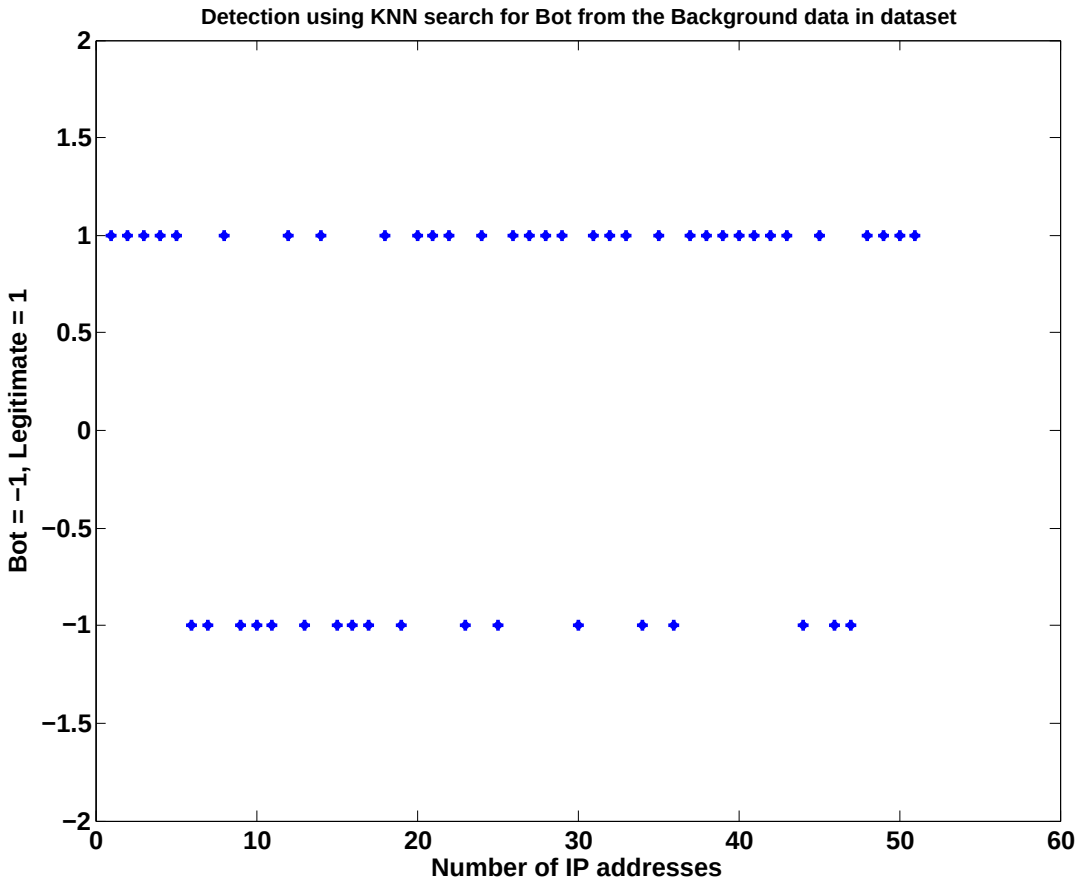

Figure 7.8: The labels after the detection of bot and regular IP addresses from the IP addresses in Background data in the dataset using KNN search.

7.10 Concluding Remarks

Bayesian mechanisms and learning methods have been utilized in this chapter to allocate the power in the wireless networks where malicious users exist. With partial information about the user behavior, the Bayesian game using pricing is analyzed. Network with arbitrary number of malicious users is considered and BNE points are obtained. It is observed that the BNE points of the pricing game is not unique due to the nonlinear non-convex nature of the BRs of the users. The user misbehavior is detected by learning anomalies in the utilities and the malicious users are priced higher using the probabilistic statistic from the detection. Then a CDMA system is considered where each user in the system has an SINR-based QoS requirement. Numerically the BNE of the pricing game is compared with the NE of complete information case.

8 Summary and Future Directions

In this thesis, we have designed decentralized pricing and centralized auction mechanisms for efficient power and spectrum allocation in interference constrained systems. We have first designed pricing mechanism for efficient power allocation in a multiuser multicarrier wirelss system uplink with sum transmission power constraint over the users and carriers. The efficient prices for price taking users are obtained as functions of Legrange multipliers of the multicarrier constraints and the received SINR vector at the base station. We have also considered multihop heterogeneous wireless networks and pricing functions for different Femto cell relays have been designed. We have proposed a concept of interference tax which should be collected by an external regulator from the relays. Unlike the wireline case, the charging function for efficient allocation has been observed to be a function of the transmission power as well as the traffic flow rate.

In the location privacy mechanism for mobile commerce, the total budget required to obtain the desired minimum level of granularity of location information from all the users has been obtained. As expected, the granularity of location information selected by the users decreases with increasing risk factor. We have used real GPS data on location information to obtain the simulation results. A map of users has been constructed from their reported granularity level of information and the actual GPS data. An iterative algorithm has been proposed for the implementation of pricing mechanisms and its convergence has been proved. Then a regression learning method has been used by the designer to learn the utility functions of users from their actions, unlike in direct mechanisms where the designer asks the users to report their utility functions. In the simulations, we have shown that the functions can be approximated well by the Gaussian regression method.

A new modeling of malicious user utility function has been proposed and a metric PoM for quantifying the effect of malicious users has been defined. The PoM for pricing and auction mechanisms has been obtained. We have observed a Braess type paradox in one case, where the presence of malicious users improve the social welfare of a mechanism. Next one of the mechanism for additive sharing has been proven to be ϵ-group strategy-proof against the collusion behavior of malicious users. Both the pricing and auction mechanisms have been extended for countering the malicious users. Next, we have relaxed the assumption that the users and the designer know the nature of users and designed Bayesian mechanisms. The conditions under which the uncertainty about the nature of the users is beneficial for the regular users and designer have been obtained by comparing to the complete information case. We have also obtained a truthful Bayesian mechanism for wireless networks with malicious users, based on the allocation and pricing of the dAGVA mechanism. In addition, we have observed through simulations that when the malicious user is originally more malicious, it receives increasing cost from the

truthful Bayesian mechanism for reporting as a regular user. We have used hypothesis testing and machine learning methods to detect the bots in a wireless network. Three machine learning techniques, SVM, Naive Bayes and KNN have been compared using performance matrices. Finally, the optimal prices with malicious users for the complete information case where each user submits an SINR-based QoS requirement are obtained. Then these prices have been modified with Bayesian information.

We have not addressed in detail the problem of imperfect channel knowledge in this thesis, which is important for the practicality of the mechanisms proposed in this thesis to wireless systems. The prices proposed in the Section 3.2 can be implemented by measuring the received power and received SINR at the receiver in the base station. In the remaining part of the thesis, the channel knowledge is required for implementation of the mechanisms. Therefore, the scenario where the users report false channel gains to strategically influence the resource allocation is an important direction [117].

Bringing more dynamics to the system via stochastic games [88] is an interesting direction for future work. Especially, in the context when users have imperfect information [108]. The effect of malicious users in hierarchical games [63] is another interesting future direction.

Publication List

This list collects the author's publications on the topics of this thesis which have appeared in conference proceedings or journals. They are also included in the Bibliography.

- A. K. Chorppath and T. Alpcan, Trading privacy with incentives in mobile commerce: A game theoretic approach, *Elsevier Pervasive and Mobile Computing*, August 2012.
- A. K. Chorppath, T. Alpcan, and H. Boche, Adversarial Behavior in Network Games, *Springer Dynamic Games and Applications,* Vol. 5, Issue. 1, March, 2015.
- A. K. Chorppath, F. Shen, T. Alpcan, E. A. Jorswieck and H. Boche, Bayesian Mechanisms and Learning for Wireless Networks Security with QoS Requirements. *In Proc. of IEEE International Conference on Communications (ICC),* June 2015, London, United Kingdom.
- A. K. Chorppath, T. Alpcan, and H. Boche, Bayesian Mechanisms for Wireless Network Security. *In Proc. IEEE International Conference on Communications (ICC)*, June 2014, Sydney, Australia.
- A. K.Chorppath, E. M. Yeh and H. Boche, Pricing Games in Multihop Wireless Networks under Interference Constraints. *In Proc. The 5th International Workshop on Indoor and Outdoor Small cells (IOSC)*, Wiopt, Hammamet, Tunisia, May, 2014.
- F. Shen, E. Jorswieck, A. K. Chorppath and H. Boche, Pricing for Distributed Resource Allocation in MAC without SIC under QoS Requirements with Malicious Users. *WNC, Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'14)*, Hammamet, Tunisia, May, 2014.
- A. K. Chorppath and T. Alpcan, Learning User Preferences in Mechanism Design. *In Proc. 50th IEEE Conference on Decision and Control and European Control Conference, CDC ECC '11*, Florida, USA, December 2011.
- A. K. Chorppath and T. Alpcan, A Privacy Mechanism for Mobile Commerce. *In Proc. 2nd IEEE International Workshop on Data Security and Privacy in wireless Networks, DSPAN'11*, June 20, 2011, Lucca, Italy.
- A. K. Chorppath and T. Alpcan, Mechanism design for energy efficiency in wireless networks. *In Proc.the 7th Intl. Workshop on Resource Allocation and Cooperation in Wireless Networks (RAWNET/WNC3)*, WiOpt, Princeton, USA, May 2011.

- A. K. Chorppath and T. Alpcan, Adversarial behavior in network mechanism design. *In Proc. of 4th Intl. Workshop on Game Theory in Communication Networks, Gamecomm*, ENS, Cachan, France, May 2011.
- A. K. Chorppath, T. Alpcan, and H. Boche, Pricing mechanisms for multi-carrier wireless systems. *In Proc. IEEE Intl. Dynamic Spectrum Access Networks Symp., DySPAN,* Aachen, Germany, May 2011.

Bibliography

[1] D. Acemoglu and A. Ozdaglar. Competition and efficiency in congested markets. *Mathematics of Operations Research*, 32(1):1 – 31, 2007.

[2] T. Alpcan and T. Başar. A Utility-Based Congestion Control Scheme for Internet-Style Networks with Delay. *IEEE Trans. on Networking*, 13(6):1261–1274, December 2005.

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

[4] T. Alpcan, H. Boche, M. Honig, and H. V. Poor, editors. *Mechanisms and Games for Dynamic Spectrum Allocation*. Cambridge University Press, 2013.

[5] 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.

[6] 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*, pages 1 –6, oct. 2011.

[7] G. Aryal and M. F. Gabrielli. Revenue under collusion-proof auctions. *Available at SSRN*, 2012.

[8] R. J. Aumann. Correlated equilibrium as an expression of bayesian rationality. *Econometrica*, 55(1):1 – 18, 1987.

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

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

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

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

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

[14] M.-F. Balcan, A. Blum, J. D. Hartline, and Y. Mansour. Reducing mechanism design to algorithm design via machine learning. *J. Comput. Syst. Sci.*, 74:1245–1270, December 2008.

[15] A. Baliga and B. Coskun. Mobile botnet mitigation, june 2012. US Patent App. 12/962,940.

[16] M. Bennis and M. Debbah. On spectrum sharing with underlaid femtocell networks. In *Second IEEE Workshop on Indoor and Outdoor Femto Cells (in conjunction with IEEE PIMRC'10), Istanbul*, Istanbul, Turkey, 2010.

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

[18] H. Boche, S. Naik, and T. Alpcan. A unified mechanism design framework for networked systems. Technical report, arXiv:1009.0377[cs.GT], September 2010.

[19] H. Boche, S. Naik, and T. Alpcan. Universal pricing mechanism for utility maximization for interference coupled systems. In *European Wireless Conference (EW)*, pages 661 –666, April 2010.

[20] H. Boche, S. Naik, and T. Alpcan. Characterization of convex and concave resource allocation problems in interference coupled wireless systems. *IEEE Transactions on Signal Processing*, 59(5):2382–2394, May 2011.

[21] H. Boche, S. Naik, and E. A. Jorswieck. Detecting misbehavior in distributed wireless interference networks. *Wireless Networks*, 19(5):799–810, 2013.

[22] H. Boche and M. Schubert. A calculus for log-convex interference functions. *Information Theory, IEEE Transactions on*, 54(12):5469 –5490, dec. 2008.

[23] H. Boche and M. Schubert. Concave and convex interference functions-general characterizations and applications. *Signal Processing, IEEE Transactions on*, 56(10):4951 –4965, oct. 2008.

[24] H. Boche and M. Schubert. The structure of general interference functions and applications. *Information Theory, IEEE Transactions on*, 54(11):4980 –4990, nov. 2008.

[25] H. Boche and M. Schubert. A unifying approach to interference modeling for wireless networks. *Signal Processing, IEEE Transactions on*, 58(6):3282 –3297, june 2010.

[26] H. Boche and M. Schubert. A generalization of nash bargaining and proportional fairness to log-convex utility sets with power constraints. *IEEE Transactions on Information Theory*, 57(6):3390–3404, 2011.

[27] 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*, pages 1207–1214, Hyderabad, India, 2007.

[28] Q. Cao, H. Zhao, and Y. Jing. Power allocation and pricing in multiuser relay networks using stackelberg and bargaining games. *Vehicular Technology, IEEE Transactions on*, 61(7):3177–3190, Sept 2012.

[29] J. Chen and S. Micali. Collusive dominant-strategy truthfulness. *Journal of Economic Theory*, 147(3):1300 – 1312, 2012.

[30] L. Chen, L. Libman, and J. Leneutre. Conflicts and incentives in wireless cooperative relaying: A distributed market pricing framework. *Parallel and Distributed Systems, IEEE Transactions on*, 22(5):758–772, May 2011.

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

[32] 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.

[33] A. K. Chorppath and T. Alpcan. Mechanism design for energy efficiency in wireless networks. In *In Proc. of the 7th Intl. Workshop on Resource Allocation and Cooperation in Wireless Networks (RAWNET/WNC3)*, Princeton, USA, May 2011.

[34] A. K. Chorppath and T. Alpcan. Trading privacy with incentives in mobile commerce: A game theoretic approach. *Pervasive and Mobile Computing*, 9(4):598 – 612, 2013.

[35] A. K. Chorppath, T. Alpcan, and H. Boche. *Mechanisms and Games for Dynamic Spectrum Allocation*, chapter Games and Mechanisms for Networked Systems: Incentives and Algorithms. In Alpcan et al. [4], 2013.

[36] A. K. Chorppath, T. Alpcan, and H. Boche. Bayesian mechanisms for wireless network security. In *IEEE International Conference on Communications (ICC)*, Sydney, Australia, June 2014.

[37] A. K. Chorppath, T. Alpcan, and H. Boche. Adversarial behavior in network games. *Dynamic Games and Applications*, 5(1):26–64, 2015.

[38] 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*, 8(3):520–531, July 2011.

[39] 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.

[40] A. A. Daoud, T. Alpcan, S.Agarwal, and M. Alanyali. A stackelberg game for pricing uplink power in wide-band cognitive radio networks. In *47th IEEE Conference on Decision and Control, 2008. CDC 2008.*, pages 1422 – 1427, 9-11 December 2008.

[41] C. d'Aspremont and L.-A. Grard-Varet. Incentives and incomplete information. *Journal of Public Economics*, 11(1):25 – 45, 1979.

[42] O. Dekel, F. Fischer, and A. D. Procaccia. Incentive compatible regression learning. In *Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms*, SODA '08, pages 884–893, Philadelphia, PA, USA, 2008. Society for Industrial and Applied Mathematics.

[43] T. Elkourdi and O. Simeone. Femtocell as a relay: An outage analysis. *Wireless Communications, IEEE Transactions on*, 10(12):4204–4213, 2011.

[44] M. Feily, A. Shahrestani, and S. Ramadass. A survey of botnet and botnet detection. In *Third International Conference on Emerging Security Information, Systems and Technologies*, June 2009.

[45] N. Feng, S. C. Mau, and N. B. Mandayam. Pricing and power control for joint user-centric and network-centric resource allocation. *IEEE Transactions on Communications*, 52(9), 2004.

[46] W. Feng and J. M. H. Elmirghani. Lifetime evaluation in energy-efficient rectangular ad hoc wireless networks. *Int. J. Commun. Syst.*, 23(12):1500–1520, Dec. 2010.

[47] S. García. Malware capture facility project, dataset ctu-malware-capture-botnet-43. In *Czech Technical University (CVUT)*, Prague, Czech Republic, December 2013.

[48] D. Garg, Y. Narahari, and S. Gujar. Foundations of Mechanism Design: A Tutorial Part 1 - Key Concepts and Classical Results. *Sadhana*, 33(3):83–130, April 2008.

[49] G. Gu, R. Perdisci, J. Zhang, and W. Lee. Botminer: Clustering analysis of network traffic for protocol- and structure-independent botnet detection. In *Proceedings of the 17th Conference on Security Symposium*, SS'08, pages 139–154, Berkeley, CA, USA, 2008. USENIX Association.

[50] G. Gu, J. Zhang, and W. Lee. Botsniffer: Detecting botnet command and control channels in network traffic. In *Proc. 15th Annual Network and distributed System Security Symposium (NDSS08)*, 2008.

[51] C. Gueguen, A. Rachedi, and M. Guizani. Incentive scheduler algorithm for cooperation and coverage extension in wireless networks. *Vehicular Technology, IEEE Transactions on*, 62(2):797–808, Feb 2013.

[52] M. T. Hajiaghayi, R. Kleinberg, and D. C. Parkes. Adaptive limited-supply online auctions. In *In Proceedings of the 5th ACM Conference on Electronic Commerce*, pages 71–80. ACM Press, 2004.

[53] J. C. HARSANYI. Games with incomplete information played by 'bayesian' players. *Management Science, Theory Series*, 14(3), 1967.

[54] 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*, STOC '06, pages 89–98, New York, NY, USA, 2006. ACM.

[55] J. Hirshleifer, A. Glazer, and D. Hirshleifer. *Price Theory and Applications Decisions, Markets, and Information.* Cambridge, U.K.: Cambridge Univ. Press, 2005.

[56] H.Moulin and S.Shenker. Strategyproof sharing of submodular costs: budget balance versus efficiency. *Journal on economic theory*, 18(3):511–533, August 2001.

[57] J. Huang, R. Berry, and M. Honig. Auction–based Spectrum Sharing. *ACM Mobile Networks and Applications Journal*, 24(5):405–418, June 2006.

[58] J. Huang, R. Berry, and M. Honig. Distributed Interference Compensation for Wireless Networks. *IEEE Journal on Selected Areas in Communications*, 24(5):1074–1084, May 2006.

[59] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki. Towards modeling wireless location privacy. In *In Proceedings of Privacy Enhancing Technology(PET)*, pages 59–77, 2005.

[60] P. Hui, T. Henderson, I. Brown, and H. Haddadi. *Targeted Advertising on the Handset: Privacy and Security Challenges.* Pervasive Advertising, Springer Human-Computer Interaction Series, 2011.

[61] M. Humbert, M. H. Manshaei, J. Freudiger, and J.-P. Hubaux. Tracking games in mobile networks. In *GameSec'10*, pages 38–57, 2010.

[62] N. Husted and S. Myers. Mobile location tracking in metro areas: Malnets and others. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*, CCS '10, pages 85–96, New York, NY, USA, 2010. ACM.

[63] G. Iosifidis, A. Chorppath, T. Alpcan, and I. Koutsopoulos. Incentive mechanisms for hierarchical spectrum markets. In *Network Games, Control and Optimization (NetGCooP), 2012 6th International Conference on*, pages 1–8, Nov 2012.

[64] R. Johari. *Efficiency Loss in Market Mechanisms for Resource Allocation.* PhD thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts, United States, June 2004.

[65] 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*, 50(11):1712–1724, November 2005.

[66] E. Jorswieck, H. Boche, and S. Naik. Energy-aware utility regions: Multiple access pareto boundary. *Wireless Communications, IEEE Transactions on*, 9(7):2216–2226, July 2010.

[67] S. J. Kang, Y. Won, S. Lim, and M. van der Schaar. Efficient resource management with reduced overhead information. In *in IEEE Conference on Personal, Indoor and Mobile Radio Communications*, pages 1452– 1456, September 2009.

[68] V. Kavitha, E. Altman, R. El-Azouzi, and R. Sundaresan. Fair scheduling in cellular systems in the presence of noncooperative mobiles. *IEEE/ACM Trans. Netw.*, 22(2):580–594, Apr. 2014.

[69] A. K.Chorppath, E. M. Yeh, and H. Boche. Pricing games in multihop wireless networks under interference constraints. In *IN PROCEEDINGS OF 5th International Workshop on Indoor and Outdoor Small cells (IOSC), Wiopt*, pages 404–413, Hammamet, Tunisia, 2014. IEEE.

[70] 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*, 49:237–252, 1998.

[71] E. Koutsoupias and C. Papadimitriou. Worst-case equilibria. In *IN PROCEEDINGS OF THE 16TH ANNUAL SYMPOSIUM ON THEORETICAL ASPECTS OF COMPUTER SCIENCE*, pages 404–413. Lecture Notes in computer Science, 1999.

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

[73] P. T. M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, and T. L. Porta. On cellular botnets: Measuring the impact of malicious devices on a cellular network core. In *Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, CCS09, 2009.

[74] H. Liu, B. Krishnamachari, and M. Annavaram. Game theoretic approach to location sharing with privacy in a community-based mobile safety application. In *Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems*, MSWiM '08, pages 229–238, New York, NY, USA, 2008. ACM.

[75] 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)*, pages 1550–1555, Paradise Island, Bahamas, December 2004.

[76] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, and J.-P. Hubaux. Game theory meets network security and privacy. *ACM Comput. Surv.*, 45(3):25:1–25:39, July 2013.

[77] M. Margaritidis, C. N. Ververidis, G. Xylomenos, and G. C. Polyzos. A differentiated services qos scheme preventing malicious flow behavior in mobile ad hoc networks. In *Wireless Conference 2006 - Enabling Technologies for Wireless Multimedia Communications (European Wireless), 12th European*, pages 1–7, April 2006.

[78] F. Meshkati, M. Chiang, H. Poor, and S. Schwartz. A game-theoretic approach to energy-efficient power control in multicarrier CDMA systems. *IEEE Journal on Selected Areas in Communications*, 24(6):1115–1129, June 2006.

[79] F. Meshkati, H. V. Poor, S. C. Schwartz, and N. B. Mandayam. An energy-efficient approach to power control and receiver design in wireless data networks. *IEEE TRANSACTIONS ON COMMUNICATIONS*, 53:1885–1894, 2005.

[80] S. Micali and P. Valiant. Revenue in truly combinatorial auctions and adversarial mechanism design. Technical report, MIT-Computer Science and Artificial Intelligence Laboratory, June 2008.

[81] R. Min and A. Chandrakasan. Energy-efficient communication for high density networks. In T. Basten, M. Geilen, and H. de Groot, editors, *Ambient Intelligence: Impact on Embedded Sytem Design*, pages 295–314. Springer US, 2003.

[82] J. Mitola. Cognitive radio for flexible mobile multimedia communications. *Mobile Networks and Applications,*, 6:435–441, 2001.

[83] M. Morelli, C.-C. Kuo, and M.-O. Pun. Synchronization techniques for orthogonal frequency division multiple access (ofdma): A tutorial review. *Proceedings of the IEEE*, 95(7):1394–1427, July 2007.

[84] 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.

[85] K. P. Murphy. *Machine Learning: A Probabilistic Perspective (Adaptive Computation and Machine Learning series)*. The MIT Press, Aug. 2012.

[86] R. B. Myerson. Optimal auction design. *MATHEMATICS OF OPERATIONS RESEARCH*, 6(1):58–73, February 1981.

[87] N. Netzer. An externality-robust auction. *Working Paper*, 2012.

[88] K. C. Nguyen and T. Alpcan. Stochastic games for security in networks with interdependent nodes. In *Int. Conf. on Game Theory for Networks*, 2009.

[89] K. C. Nguyen, T. Alpcan, and T. Basar. A decentralized bayesian attack detection algorithm for network security. In S. Jajodia, P. Samarati, and S. Cimato, editors, *Proceedings of The Ifip Tc 11 23rd International Information Security Conference*, volume 278 of *IFIP The International Federation for Information Processing*, pages 413–428. Springer US, 2008.

[90] D. C. Parkes and L. H. Ungar. Iterative combinatorial auctions: Theory and practice. In *Proceedings of the Seventeenth National Conference on Artificial Intelligence and Twelfth Conference on Innovative Applications of Artificial Intelligence*, pages 74–81. AAAI Press, 2000.

[91] N. Rama Suri and Y. Narahari. Broadcast in ad hoc wireless networks with selfish nodes: A bayesian incentive compatibility approach. In *Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on*, pages 1–9, 2007.

[92] C. E. Rasmussen and C. K. I. Williams. *Gaussian Processes for Machine Learning (Adaptive Computation and Machine Learning)*. The MIT Press, 2005.

[93] S. Ren and M. van der Schaar. Revenue maximization and distributed power allocation in cognitive radio networks. In *Proceedings of the 2009 ACM workshop on Cognitive radio networks*, CoRoNet '09, pages 43–48, New York, NY, USA, 2009. ACM.

[94] J. B. Rosen. Existence and uniqueness of equilibrium points for concave n -person games. *Econometrica*, 33(3):520–534, 1965.

[95] 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*, pages 118–125, 2008.

[96] 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.

[97] S. Saad, I. Traore, A. Ghorbani, B. Sayed, D. Zhao, W. Lu, J. Felix, and P. Hakimian. Detecting p2p botnets through network behavior analysis and machine learning. In *Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on*, pages 174–180, July 2011.

[98] Y. Sagduyu, R. Berry, and A. Ephremides. MAC games for distributed wireless network security with incomplete information of selfish and malicious user types. In *GameNets'09*, pages 130–139, 2009.

[99] Y. Sagduyu, R. Berry, and A. Ephremides. Jamming games for power controlled medium access with dynamic traffic. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 1818–1822, June 2010.

[100] C. Saraydar, N. Mandayam, and D. Goodman. Efficient power control via pricing in wireless data networks. *IEEE Transactions on Communications*, 50(2):291–303, Feb. 2002.

[101] R. F. Schaefer, H. Boche, and H. V. Poor. Secure communication under channel uncertainty and adversarial attacks. *Proceedings of the IEEE*, 2015.

[102] R. F. Schaefer, H. Boche, and H. V. Poor. Super-activation as a unique feature of secure communication in malicious environments. *IEEE Transactions on Information Forensics and Security*, July 2015.

[103] S. Shakkottai, R. Srikant, A. Ozdaglar, and D. Acemoglu. The price of simplicity. In *Forty-First Asilomar Conference on Signals, Systems and Computers, ACSSC 2007*, pages 1450 – 1454, Pacific Grove, CA, 2007.

[104] F. Shen and E. Jorswieck. Universal non-linear cheat-proof pricing framework for wireless multiple access channels. *Wireless Communications, IEEE Transactions on*, 13(3):1436–1448, March 2014.

[105] F. Shen, E. Jorswieck, A. K. Chorppath, and H. Boche. Pricing for distributed resource allocation in mac without sic under qos requirements with malicious users. In *WNC, Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'14)*, Hammamet, Tunisia, May 2014.

[106] Z. Shen, A. Papasakellariou, J. Montojo, D. Gerstenberger, and F. Xu. Overview of 3gpp lte-advanced carrier aggregation for 4g wireless communications. *Communications Magazine, IEEE*, 50(2):122–130, February 2012.

[107] H. Shinsuke and R. Prasad, editors. *Multicarrier Techniques for 4G Mobile Communications*. Artech House, Inc., Norwood, MA, USA, 1st edition, 2004.

[108] S. Shiva, S. Roy, H. Bedi, D. Dasgupta, and Q. Wu. Stochastic games for security in networks with interdependent nodes. In *The 5th International Conference on Information-Warfare and Security*, 2010.

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

[110] K. Steiglitz, J. Morgan, and G. Reis. The spite motive and equilibrium behavior in auctions. *Contributions to Economic Analysis and Policy*, 2(5), 2003.

[111] S.Theodorakopoulos and J. S. Baras. Game theoretic modeling of malicious users in collaborative networks. *IEEE Journal on selected areas in communications*, 26(7):1317–1327, August 2008.

[112] W. Vickrey. Counterspeculation, auctions and competitive sealed tenders. *Journal of Finance*, 16(1):8–37, 1961.

[113] I. Vural and H. Venter. Mobile botnet detection using network forensics, 2010.

[114] F. Wang, M. Krunz, and S. Cui. Price-based spectrum management in cognitive radio networks. *IEEE Journal of Selected Topics in Signal Processing*, 2(1):74–87, February 2008.

[115] Q. Wu, S. Shiva, S. Roy, C. Ellis, and V. Datla. On modeling and simulation of game theory-based defense mechanisms against dos and ddos attacks. In *Proceedings of the 2010 Spring Simulation Multiconference*, SpringSim '10, pages 159:1–159:8, San Diego, CA, USA, 2010. Society for Computer Simulation International.

[116] Y. Xi and E. M. Yeh. Pricing, competition, and routing for selfish and strategic nodes in multi-hop relay networks. In *INFOCOM'08*, pages 1463–1471, 2008.

[117] H. Xiao and E. Yeh. The impact of incomplete information on games in parallel relay networks. *IEEE Journal on Selected Areas in Communications*, 30(1):176–187, 2012.

[118] 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*, pages 47–56, 2005.

[119] R. Yates. A framework for uplink power control in cellular radio systems. *Selected Areas in Communications, IEEE Journal on*, 13(7):1341–1347, sep 1995.

[120] W. Yu, W. Rhee, S. Boyd, and J. M. Cioffi. Iterative water-filling for gaussian vector multiple-access channels. *IEEE Transactions on Information Theory*, 50(1):145–152, January 2004.

[121] Y. Zheng, Q. Li, Y. Chen, X. Xie, and W.-Y. Ma. Understanding mobility based on gps data. In *Proceedings of ACM conference on Ubiquitous Computing (UbiComp 2008)*, pages 312–321, Seoul, Korea, 2008.

[122] Y. Zheng, X. Xie, and W.-Y. Ma. Geolife: A collaborative social networking service among user, location and trajectory. *IEEE Data Engineering Bulletin*, pages 32–40, 2010.

[123] Y. Zheng, L. Zhang, X. Xie, and W.-Y. Ma. Mining interesting locations and travel sequences from gps trajectories. In *Proceedings of International conference on World Wild Web (WWW 2009)*, pages 791–800, Madrid Spain, 2009.

[124] Z. Zhu, G. Lu, Y. Chen, Z. J. Fu, P.Roberts, and K. Han. Botnet research survey. In *Proc. 32nd Annual IEEE International Conference on Computer Software and Applications (COMPSAC '08)*, pages 967–972, 2008.