Bayesian Mechanisms and Learning for Wireless Networks Security with QoS Requirements

Anil Kumar Chorppath[†], Fei Shen[*], Tansu Alpcan[‡], Eduard Jorswieck[*]and Holger Boche[†]
[*]Communications Theory, Communications Laboratory
Technical University of Dresden, Germany
E-mail: {Fei.Shen, Eduard.Jorswieck}@tu-dresden.de
[†] Institute of Theoretical Information Technology, Technical University of Munich, Germany
E-mail: {anil.chorppath, boche}@tum.de
[‡] The University of Melbourne, Australia
Email: tansu.alpcan@unimelb.edu.au

***Abstract*—When there are strategic and malicious users in a wireless network, the resource allocation is complicated due to the information limitation about the nature of users and network parameters. Bayesian games are appropriate tools to analyze the network resource allocation with heterogeneous users. We consider a scenario with arbitrary number of malicious users in the network, in which individual users gather probabilistic information about the density of malicious users. Users and the base station observe the network over a long time period and modify their actions accordingly. The power allocation in wireless networks which we consider in this paper, is subject to Quality of Service (QoS) requirements. We consider Bayesian pricing mechanisms where the prices are modified using the Bayesian information about types of the users to satisfy the QoS requirements. We also give detection methods based on regression learning algorithms which are used for forming the probability of a user being malicious. The utilities of the users are formed by observing the power strategies of the users and the anomalies are detected. We obtain numerically, the Bayesian Nash Equilibrium (BNE) points of the Bayesian games. We also evaluate the effect of incomplete information on the satisfaction of the QoS requirements of the users in the mechanisms. These mechanisms are with prices which were originally developed for networks with complete information.**

I. Introduction

There has been an increasing interest to analyse the security problems using game theory [1]. 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 int the network [2]. The information available in the hand of base station for the resource allocation is limited in most realistic scenarios [3]. The users are not price anticipating in a distributed network in which 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. Hence, they cannot anticipate the exact impact of their action on the pricing function and they just adopt a best response strategy by taking the price as a constant given by the designer. The users only report their QoS requirements and take Best Response(BR) power strategy.

The users in the wireless systems are rational agents in the game theoretic sense that they aim to maximize their own utilities. It is possible that the mobiles which share the same spectrum have incentives to misrepresent their private information for better utilities. Such private information includes channel state information (CSI), user preferences and the nature of users [4]. Therefore to supervise and influence the operation of the system is an important task of the system operator [1], [5].

We analyze Bayesian games in which users have a probabilistic distribution over the type of the other users. The utility of a user 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 with QoS requirements is quantified within a Bayesian framework [6]. In our work, we develop the distributed power allocation with individual pricing for the general MAC system without successive interference cancellation (SIC). 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. Each user has a rate-based QoS requirement, which is guaranteed through the prices in the non-cooperative game [7]. The work in [3] which proposed Bayesian mechanisms for net utility maximization is extended with QoS requirement for the users.

Nowadays the wireless communications and networking practices are tightly coupled with economic considerations [8]. Particularly, pricing has been successively applied into the wireless networks to enforce the system efficiency. The interference and resource allocation on the physical layer of the wireless communications can be managed by smart pricing adaptation [9]. The prices in the wireless system refer more to the control signal as some virtual currency in the utility functions of each user [10]. A strategy-proof pricing mechanism is the one in which with the proper

The work by Anil Kumar Chorppath and Holger Boche is partly supported by the COIN project by the German National Science Foundation (DFG) BO 1734/20-1. This work of Fei Shen and Eduard Jorswieck is partly supported by the DFG under grant Jo 801/5-3. Tansu Alpcan's work is in part supported by the ARC DP 140100819

978-1-4673-6432-4/15/$31.00 ©2015 IEEE

price adaptation, no user in the system behave maliciously to others. We propose malicious behavior resistant Bayesian mechanisms [11] which have a designer (network) who designs prices based on information expressed. We extend the work in [12] to an incomplete information case where the malicious behavior is countered without explicit detection of malicious users by learning their nature. The designer knows the probability of malicious user's existence and counters them by updating the prices using the probabilistic information in the pricing mechanism. The additional pricing by the designer and the uncertainty about the nature of users counter malicious activities.

In mobile networks, Gaussian process regression is used to model spatial functions or other functions [13]. The paper [14] utilizes Gaussian process regression learning techniques to infer general user utilities to maximize the social welfare by a designer in a mechanism design setting. In pricing mechanisms, the price taking players are charged with the appropriate value of Lagrange multiplier which corresponds to the marginal utility functions of the users. In [15], the condition for correctly detecting malicious links in a wireless network is obtained based on the global dependency matrix, which captures the effect of interference coupling in the system. In this paper, we use regression learning methods to infer user utilities of the regular and malicious users by a designer to satisfy the QoS requirements. Such learning schemes decrease the communication requirements considerably and allow usage of successive scalar bids or actions from the users, even though the users have infinitely-dimensional utility functions. We apply the regression learning technique to pricing mechanisms, to learn the utility function of regular and malicious users and then the malicious users are detected by observing the anomalies in utility functions. The detection helps to develop probability beliefs of each user in the network being malicious which in turn is used for Bayesian pricing.

The contributions of the paper:

1) In contrast to [7], the users do not know the nature of other users. They take actions according to probability beliefs about the types of others but with QoS requirements.
2) Furthermore, the designer does not know the identities of the malicious users for determining the prices. Therefore, the designer acts with Bayesian information for the implementation of differentiated pricing.
3) The results in [3] are extended to SINR pricing, Shannon rate as utility function, QoS requirements and arbitrary number of malicious users.
4) The designer learns the utility function of regular and malicious users. Then the malicious users are detected by observing the anomalies in utility functions.

II. Bayesian Game Model

The model we present next is based upon the one in [3] and is partially repeated here for the sake of completeness. We denote vectors with block letters. The following Table I provides the notations and variables used in the paper. At

TABLE I: Table of Notations

Parameter	Description
$N; N^m$	Total number of users; Total number of malicious users
x_i	Received power user i in the pricing game
$\mathcal{X}$	The decision space of all users
$\underline{u}_i$	QoS requirement of user i
C_i	Payment of user i
γ_i	SINR of user i
P_i	Price per unit SINR of user i
U_i	Utility of user i
J_i	Cost of user i
B	Energy cost per unit transmitted power
h_i	Channel gain of user i
ψ^s	Probability that the other user is malicious for a regular user
ψ^m	Probability that the other user is regular for a malicious user
$\mu^s(N, N^m)$	Joint pmf of N and N^m as observed by regular user
$\mu^m(N, N^m)$	Joint pmf of N and N^m as observed by malicious user
$\mu^d(N, N^m)$	Joint pmf of N and N^m as observed by the designer
ψ_i^d	Probability that user i is malicious as observed by the designer

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

$$\mathbf{x} = [x_1, \ldots, x_N] \in \mathcal{X}$$

where $\mathcal{X} \in \Re^N$ is the decision space of all users. Let

$$\mathbf{x}_{-i} = [x_1, \ldots, x_{i-1}, x_{i+1}, \ldots x_N] \in \mathcal{X}_{-i},$$

be the profile of decision variables of users other than i^{th} user and $\mathcal{X}_{-i}$ is the respective decision space. x_i is the received power of user i in the wireless network. Let $\mathcal{B}$ be the set of malicious users with N^m elements and $\mathcal{S}$ is the set of regular users.

Assumption II.1. This paper assumes that the strategy space $\mathcal{X}$ has scalar decision variables, is compact, convex and has

a nonempty interior.

We consider a CDMA system, for which the received SINR of a user is given by

$$\gamma_i(\mathbf{x}) = \frac{h_i x_i}{I_i(\mathbf{x}_{-i})} = \frac{h_i x_i}{\frac{1}{L}\sum_{j\neq i} h_j x_j + \sigma^2}, \qquad (1)$$

where h_i is the channel gain, L is the bandwidth and σ^2 denotes noise power. L is taken as 1 in the model of [7].

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

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

Assumption II.2. The utility function of the i^{th} user, $U_i(\mathbf{x})$, is jointly continuous in all its arguments and twice continuously differentiable, non-decreasing and strictly concave in x_i.

The Shannon rates are considered as the utility functions, i.e.,

$$U_i(x_i, x_{-i}) = \log\left(1 + \gamma_i(\mathbf{x})\right) \quad \forall i \in \mathcal{A}. \qquad (2)$$

The QoS requirements are satisfied if

$$U_i(x_i, x_{-i}) \geq \underline{u}_i, \quad \forall i \in \mathcal{A}. \qquad (3)$$

where $\underline{u}_i$ is the QoS (rate) requirement of user i.

The modified utility function [12] to model malicious users is obtained by a convex combination of user utilities

$$U_i^m(\gamma_i(\mathbf{x})) = U_i(\gamma_i(\mathbf{x})) + \theta_i \sum_{k\in S} U_k(\gamma_k(\mathbf{x})), \qquad (4)$$

where θ_i is the parameter between -1 and 0. The variable θ captures the range of behavior of a user from malicious to selfish. The first term on the right-hand side is the self utility and the second term captures the malicious goal of the user. For a malicious user, the variable $\theta < 0$ and is called *degree of maliciousness*. We assume that malicious users do not gain anything by harming each other.

The designer $\mathcal{D}$ devises a **mechanism**, $\mathcal{M} = \langle\, N, N^m, \mathcal{X}, \mathbf{J}\,\rangle$, which is represented by the mapping $\mathcal{M} : \mathcal{X} \to \Re^N$, by introducing incentives in the form of *rules and prices* to users. $\mathbf{J}$ is the set of cost functions of the users. Let $C_i(\mathbf{x})$ be the total payment by the i^{th} user to the mechanism.

Assumption II.3. The payment function of the i^{th} user, $C_i(\mathbf{x})$, is jointly continuous in all its arguments and twice continuously differentiable, non-decreasing and convex in x_i.

We consider SINR pricing in this paper,

$$C_i(\mathbf{x}) = \beta_i \gamma_i(\mathbf{x}), \ \forall\ i.$$

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.

Now 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. The cost function of the regular user will be,

$$\begin{aligned} J_i^s(x^s, x^m) &= \sum_{N^m=0}^{N} \mu^s(N, N^m)(\beta_i \gamma_i^s(N, N^m) + B\frac{x_i^s}{h_i} \\ &- U(\gamma_i^s(N, N^m)). \end{aligned} \qquad (5)$$

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.

The maliciousness term is the utility function of user i is replaced in [7] with the SINR of user i. The reason is that the malicious user affects all the other users with his SINR. Then the cost function of the malicious user for the symmetric case with $\theta_i = \theta^m,\ \forall\ i$ is

$$\begin{aligned} J^m(\mathbf{x}) &= \sum_{N^m=0}^{N} \mu^m(N, N^m)(\alpha(\beta\gamma^m(N, N^m) + B\frac{x^m}{h^m}) \\ &- U(\gamma^m(N, N^m)) + \theta^m \gamma^m(N, N_m)), \end{aligned} \qquad (6)$$

where α_i is the parameter which indicates how much the malicious user i is sensitive towards the payment. Some malicious users would like to disrupt the network even by taking the chance of getting detected and for them $\alpha = 0$. A malicious user does not gain anything by creating interference to other malicious users. For this malicious users need to spend more energy and pay price for the extra power. Therefore, when two malicious users encounter each other in the game they have only payment and energy cost.

The Bayesian Nash Equilibrium (BNE) of the bayesian game is the solution point where no player gains anything by changing their own strategies. The BNE with heterogeneous users can be obtained from the intersection of the best responses of all users, given by

$$x_i^* \in \arg\min_{x_i} J_i^m(x_i, \mathbf{x}_{-i}^*),\ \forall\ i. \qquad (7)$$

III. Bayesian Pricing Game Analysis

In this section, we analyse the Bayesian game for which the model is presented in the previous section. We consider symmetric assumption where each user believes that other nodes of same type choose the same strategy. For an arbitrary number of malicious users with symmetry assumption, the cost function of a user, if it is regular, is given in equation (5) and if malicious, in equation (6). The following proposition gives the BNE power strategies of the regular user and the malicious user with Shannon rate utilities.

Proposition III.1. *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* $x^s \geq 0,\ x^m \geq 0$*;*

$$\sum_{N^m=0}^{N} \mu^s(N, N^m)(\gamma' + \frac{B}{h^s} - \frac{N^m h^m x^m + L\sigma^2}{\gamma^1 \left((N - N^m - 1)h^s x^s + N^m h^m x^m + L\sigma^2\right)^2}) = 0,$$

where $\gamma' = \dfrac{\beta N^m h^m x^m + L\sigma^2}{\left((N - N^m - 1)h^s x^s + N^m h^m x^m + L\sigma^2\right)^2}$ *and* $\gamma^1 = (1 + \gamma^m(N, N_m))$*, and*

$$\sum_{N^m=0}^{N} \mu^m(N, N^m)L(\gamma'_\theta + \frac{B}{h^m} - \frac{(N - N^m)h^s x^s + L\sigma^2}{\gamma^1 \left((N - N^m)h^s x^s + (N^m - 1)h^m x^m + L\sigma^2\right)^2}) = 0,$$

where $\gamma'_\theta = \dfrac{(\alpha\beta + \theta^m)((N - N^m)h^s x^s + L\sigma^2)}{\left((N - N^m)h^s x^s + (N^m - 1)h^m x^m + L\sigma^2\right)^2}$.

Proof: The BR of a regular user is obtained from the cost function in equation (5). Similarly, the BR of malicious users is obtained from the equation (6). From the definition of BNE in (7), we obtain the solution in the proposition. ■

IV. Differentiated Pricing 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. The power allocation to achieve the QoS requirement $\underline{u}_i$ of each user is proved in [9] 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 [7] as

$$\beta_i = \frac{h_i}{2^{\underline{u}_i}},\ \forall\ i. \tag{8}$$

First we discuss the pricing with complete information and extend it to Bayesian case later.

A. 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 [7]. With the individual price $\beta_i = \frac{\alpha_i}{2^{\underline{u}_i}},\ \forall\ i$, the Nash equilibrium power allocation $x_i^{NE}(\theta_i)$ of each user i in the noncooperative game $\mathcal{G}$ in the general MAC system with private type θ_i is higher than or equal to x_i^U in (8), where

$$\underline{x}_i^{NE}(\theta_i, \theta_{-i}) = \frac{1 - \theta_i - 2^{-\underline{u}_i}}{\alpha_i \sum_{j=1}^{N}(2^{-\underline{u}_j} + \theta_j) - N + 1},\ \forall\ i. \tag{9}$$

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 (9) but with $\theta_i = 0,\ \forall\ i$.

In differentiated pricing, the malicious user is punished with price β^m and the selfish user by β^s. In the N-user non-cooperative game $\mathcal{G}$ of general MAC system, no malicious user will have incentive to behave maliciously if the punishment price [7] β_i^m is given by

$$\beta_i^m \geq \beta_i^s - \theta_i h_i,\ \forall\ i. \tag{10}$$

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.

B. 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 [15]. 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;

$$\beta_i^m = \frac{h_i}{2^{\underline{u}_i}} - \psi_i^d \theta_i^d h_i. \tag{11}$$

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

$$\begin{aligned} J_i &= B\frac{x_i^s}{h_i} + \psi^s((\beta_i^s - \psi_i^d\theta_i^d h_i)\gamma_i^{sm}) \\ &- U_i\left(\gamma_i^{sm}\right)) + (1 - \psi^s)((\beta_i^s - \psi_i^d\theta_i^d h_i)\gamma_i(x_i^s, x_j^s) \\ &- U_i\left(\gamma_i(x_i^s, x_j^s)\right)), \end{aligned} \tag{12}$$

and for malicious user

$$\begin{aligned} J_i^m &= \alpha_i B\frac{x_i^m}{h_i} + \psi^m(\alpha_i(\frac{h_i}{2^{\underline{u}_i}} - \psi_i^d\theta_i^d h_i)\gamma_i(x_i^m, x_j^s) \\ &- U_i(x_i^m, x_j^s) - \theta_i\gamma_i(x_i^m, x_j^s)) \\ &+ (1-\psi^m)\alpha_i(\frac{h_i}{2^{\underline{u}_i}} - \psi_i^d\theta_i^d h_i)\gamma_i(x_i^m, x_j^m), \quad (13) \end{aligned}$$

where $\gamma_i^{sm} = \gamma_i(x_i^s, x_j^m)$. The BNE can be obtained from these cost functions.

In the next Section IV-C, 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 (11). Then we compare the Bayesian case, to the complete information case.

C. Detection and Pricing by Learning Utilities

The designer needs to know the utility functions to find the prices as in equation (10), in the previous sections. Also the designer needs to know the identities of the malicious user. In this section, regression techniques are used to learn the user private marginal utilities by the designer. The anomalies in the utility curves are used to obtain the identities of malicious users with a possible error and further for implementation of the differentiated pricing mechanism. The utility function is not assumed to be Shannon rate here and it can be any concave function. The users just give their utility requirements $\underline{u}_i,\ \forall\ i$ and take the best responses.

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

$$\min_{x_i} \quad \beta_i\gamma_i - U_i(x),$$

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

$$\beta_i\frac{d\gamma_i(x)}{dx_i} - \frac{dU_i(x)}{d\gamma_i}\frac{d\gamma_i(x)}{dx_i} = 0,\ \forall\ i \in \mathcal{A}. \quad (14)$$

Let us denote $U_i' = \dfrac{dU_i}{d\gamma_i},\ \forall\ i$. Thus,

$$\beta_i = U_i'(\gamma_i^{BR}),\ \forall\ i. \quad (15)$$

First, the designer gives sample values of prices β to all the users. Then the designer observes the NE x^{NE} and calculates the SINR at the NE, γ_i^{NE} of all the users. With different values of β, the designer can plot the curve of U_i' against γ_i. For the malicious user,

$$\beta_i = U_i'(\gamma_i^{BR}) - \theta_i\sum_{k\in S}\frac{dU_k(\gamma_k)}{d\gamma_i},\ \forall\ i. \quad (16)$$

The designer will obtain a completely different type of curve U_i' for the malicious users. The designer use this anomaly in the curve for the detection of malicious users and punish them with higher price.

From the U_i' curve, the utility function $U_i(\gamma_i)$ can be obtained by integrating. The designer objective is

$$U_i(x) \geq \underline{u}_i,\ \forall\ i.$$

Once the users give their utility requirements $\underline{u}_i,\ \forall\ i$, the designer can find the corresponding γ_i's which satisfy the designer objective with equality. The designer uses the curve obtained above using regression learning for this purpose. The price which moves the NE to the equality point can be also calculated.

The detection and pricing is part of the mechanism and can be implemented online. In addition to the pricing and channel feedback to different users the base station has a network security module which detects the malicious users and update the probability beliefs. The detections facilitate the designer to update the probability beliefs with the changing parameters in the wireless network.

V. Numerical Results

We consider an arbitrary number of malicious users out of $N = 10$ users in the pricing game in Section III. The number of malicious users are varied according to distributions $\mu^s(N, N^m)$ and $\mu^m(N, N^m)$ which are taken as binomial distribution, i.e. $\mu(N, N^m) = \binom{N}{N^m}\lambda^{N^m}(1-\lambda)^{N-N^m}$ where λ is the binomial parameter. The wireless parameters are $\sigma = 0.1$ and $L = 0.01$. The malicious user parameters are $\theta = -0.5$ and $\alpha = 0.8$. The prices taken are equal pricing given in equation (8). The utilities at BNE powers are plotted as a function of probability λ in binomial distribution belief of regular user, in Figure 1. The utility requirements are taken as $\underline{u}_i = 0.1,\ \forall\ i$. We could observe that the QoS requirement of regular users are satisfied without malicious users. When there is higher concentration of malicious users, i.e., when λ increases, utilities of regular users decrease and the QoS requirement are violated.

Next the BNE of the pricing game is compared with the NE of the complete information case, again with the price as the one in equation (8). We observe that x^{NE} is lesser for the regular user than x^U in the presence of malicious user.

VI. Conclusion

Bayesian mechanisms and learning methods are utilized to allocate the power in the wireless networks where malicious users exist. The CDMA system is considered where each user in the system has an SINR-based QoS requirement. 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 nonconvex 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. Numerically

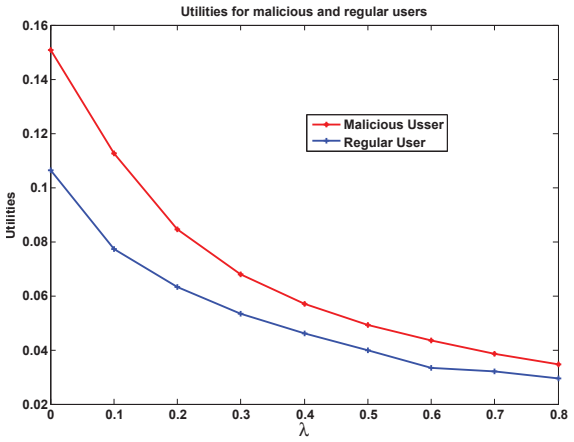

Fig. 1: The variation of utilities of users in pricing mechanism with Bayesian information in Section III, for an arbitrary number of malicious users, as a function of parameter λ in the binomial distribution.

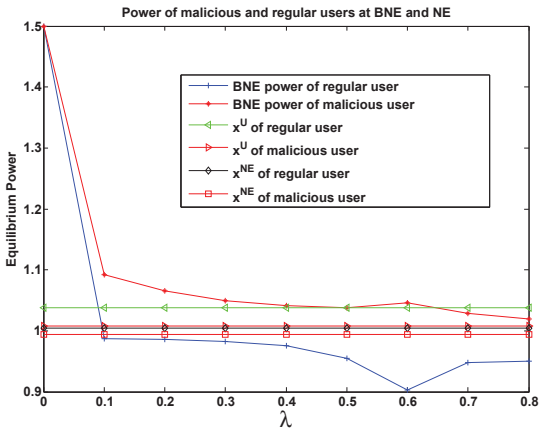

Fig. 2: BNE powers in pricing mechanism with Bayesian information in Section III for an arbitrary number of malicious users as a function of parameter λ in the binomial distribution and NE points with complete information.

the BNE of the pricing game is compared with the NE of complete information case.

References

[1] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, pp. 25:1–25:39, Jul. 2013. [Online]. Available: http://doi.acm.org/10.1145/2480741.2480742

[2] 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*, April 2006, pp. 1–7.

[3] 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.

[4] M. Biguesh and S. Gazor, "Distributed power control in cellular communication systems concerning inaccurate SINR reports," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 8, pp. 3657–3666, 2011.

[5] S. Radosavac, G. Moustakides, J. Baras, and I. Koutsopoulos, "An analytic framework for modeling and detecting access layer misbehavior in wireless networks," *ACM Trans. on Information and System Security*, vol. 11, no. 4, p. 19, 2008.

[6] X. Jin, N. Pissinou, S. Pumpichet, C. Kamhoua, and K. Kwiat, "Modeling cooperative, selfish and malicious behaviors for trajectory privacy preservation using bayesian game theory," in *Local Computer Networks (LCN), 2013 IEEE 38th Conference on*, Oct 2013, pp. 835–842.

[7] 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.

[8] J. Huang and L. Gao, "Wireless network pricing," *Synthesis Lectures on Communication Networks*, 2013.

[9] F. Shen and E. Jorswieck, "Universal non-linear cheat-proof pricing framework for wireless multiple access channels," *Wireless Communications, IEEE Transactions on*, vol. 13, no. 3, pp. 1436–1448, March 2014.

[10] C. Saraydar, N. Mandayam, and D. Goodman, "Efficient power control via pricing in wireless data networks," *Communications, IEEE Transactions on*, vol. 50, no. 2, pp. 291–303, 2002.

[11] D. Garg, Y. Narahari, and S. Gujar, "Foundations of Mechanism Design: A Tutorial Part 2 - Advanced Concepts and Results," *Sadhana*, vol. 33, no. 2, pp. 131–174, April 2008.

[12] A. K. Chorppath, T. Alpcan, and H.Boche, "Adversarial behavior in network games," *Dynamic Games and Applications*, August 2014.

[13] D. Gu and H. Hu, "Spatial gaussian process regression with mobile sensor networks," *Neural Networks and Learning Systems, IEEE Transactions on*, vol. 23, no. 8, pp. 1279–1290, Aug 2012.

[14] 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.

[15] H. Boche, S. Naik, and E. A. Jorswieck, "Detecting misbehavior in distributed wireless interference networks," *Wireless Networks*, vol. 19, no. 5, pp. 799–810, 2013.