Bayesian Mechanisms and Learning for Wireless Networks Security with QoS Requirement

Anil Kumar Chorppath, Fei Shen, Tansu Alpcan, Eduard Jorswieck and Holger Boche

Technische Universität München, Germany

The University of Melbourne, Australia and

Dresden University of Technology, Germany

ICC 2015, London

June, 2015

Motivation

- The network does not know the nature of the users.
- The malicious users act as if they are regular users so that they are not detected.
- The service provider should ensure QoS requirement of each user even in the presence of malicious users.
- The network can gather the Bayesian statistics about the nature of users over a long time period and use this to counter the malicious users.
- Key: The malicious users have different objectives compared to regular users.

Security Game

- We analyse security problems using game theory.
- The users in the wireless systems are strategic and selfish agents in the game theoretic sense that they aim to maximize their own utilities.
- We analyze Bayesian games in which users have a probabilistic distribution over the type of the other users.
- In the Bayesian pricing mechanism we design, the pricing is given such that the NE power converges to achieve the QoS requirement of each user and the malicious behavior of the users is prevented.
- A detection scheme is proposed as part of the pricing game, which eliminates the requirement of an additional scheme.

Assumptions

- Users strategies over the power which are best responses to others strategies.
- Cost functions of regular users are continuous, twice differentiable and strictly convex.
- The Channel State Information (CSI) and power strategies of all the user are common information.
- We consider a wireless network with arbitrary number of malicious users in which the network and the users have probabilistic information about the presence of malicious users.

Channel Model

- The received signal at the BS for MAC is given by

$$y = \sum_{k=1}^{K} \alpha_k x_k + n,$$

where x_k is the transmit signal of user k, n is the additive white Gaussian noise with zero-mean and variance σ^2. The channel gain of user k is denoted by $h_k = \alpha_k^2$.

- We assume the quasi-static block flat-fading channels are independent of each other and remain constant for a sufficient large number of time slots.

- We consider a CDMA system with the code gain L, for which the received SINR of a user is given by

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

Utility Model with Malicious Users

Utility function of a malicious user(Bot) is

$$U_i^m(\gamma) = U_i(\gamma_i) + \theta_i \sum_{j \in S} U_j(\gamma_j), \tag{2}$$

where θ_i is the parameter between -1 and 0 which captures the degree of maliciousness of a user.

Bayesian Game

- We consider SINR pricing in this paper,

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

- For arbitrary number of malicious users in the system, the cost function of all regular users will be,

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

For the symmetric case, the SINR of regular users become

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

- The cost function of malicious user for the symmetric case ,

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

BNE of the pricing game

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

$$\sum_{N^m=0}^{N} \mu^m(N, N^m) L(\gamma'_\theta + \frac{B}{h^m} - \frac{(N - N^m)h^s x^s + L\sigma^2}{\gamma^1 \left((N - N^m)h^s x^s + (N^m - 1)h^m x^m + L\sigma^2\right)^2}) = 0, \quad (3)$$

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

QoS Requirement

- The QoS requirement $\underline{u}_i$ of each user i in the general MAC without SIC is fulfilled if its rate $U_i \geq \underline{u}_i$, where

$$U_i = \log\left(1 + \frac{h_i x_i}{\sigma^2 + \frac{1}{L}\sum_{k \neq i} h_k x_k}\right).$$

  is the Shannon rate.

Complete Information Case: NE Power Allocation

The Nash equilibrium power allocation of each user i in the noncooperative game $\mathcal{G}$ in the general MAC system is $x_i^{NE} = \max(0, \min(\underline{x}_i^{NE}, x_i^{max}))$. With given individual prices β_i,

$$\underline{x}_i^{NE} = \frac{h_i - \beta_i}{h_i^2} \cdot \frac{1}{\sum_{j=1}^{K} \frac{\beta_j}{h_j} - K + 1}.$$

The noncooperative game $\mathcal{G}$ always admits this unique NE point.

Differentiated Pricing with QoS Requirements

- In order to determine the individual prices, $\underline{x}_i^{NE}$ should be equal to $x_i^U = \frac{B_K}{h_i} \cdot \frac{2^{\underline{u}_i}-1}{2^{\underline{u}_i}}$.

Lemma

In the K-user non-cooperative game $\mathcal{G}$ of the general MAC system, the rate requirement $\underline{u}_i$ of each user i is achieved with the NE power allocation x_i^{NE} if the individual price is

$$\beta_i = \frac{h_i}{2^{\underline{u}_i}}.$$

- For complete information case, the malicious user is punished with price β^m and the selfish user by β^s.

$$\beta_i^m \geq \beta_i^s - \theta_i h_i, \ \forall \ i. \tag{4}$$

Bayesian Pricing with QoS Requirements

- First the network creates, ψ_i^d which is the probability that user i is malicious and θ_i^d which is the estimate of degree of maliciousness of user i using a detection scheme.
- Bayesian price:

$$\beta_i^m \geq \frac{h_i}{2^{\underline{u}_i}} - \psi_i^d \theta_i^d h_i. \tag{5}$$

Detection by Learning Utilities

- The designer needs to know the utility functions of all the users and the identities of the malicious users to find the prices in the previous sections.
- We provide a method of detecting the malicious users as part of the pricing game itself.
- Regression learning techniques are used to learn the user utilities by the designer.
- Method: 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.

Anomalies in the Utilities of Malicious Users

- Let us denote $U_i' = \dfrac{dU_i}{d\gamma_i}$, $\forall\, i$. For the regular user,

$$\beta_i = U_i'(\gamma_i^{BR}),\ \forall\, i. \tag{6}$$

For the malicious user,

$$\beta_i = U_i'(\gamma_i^{BR}) - \theta_i \sum_{k \in S} \frac{dU_k(\gamma_k)}{d\gamma_i},\ \forall\, i. \tag{7}$$

- 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.

Simulation 1

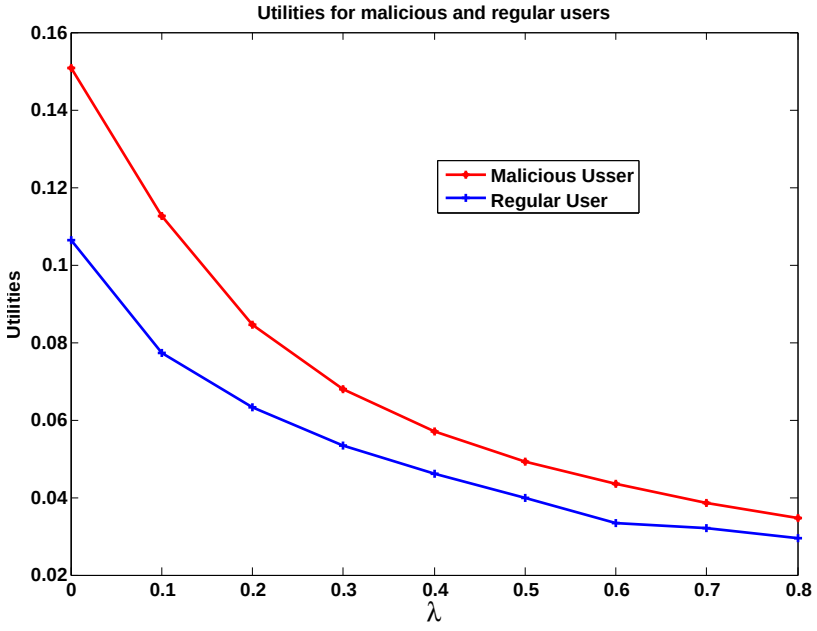

Figure: The variation of utilities of users in pricing mechanism with Bayesian information.

Simulation 2

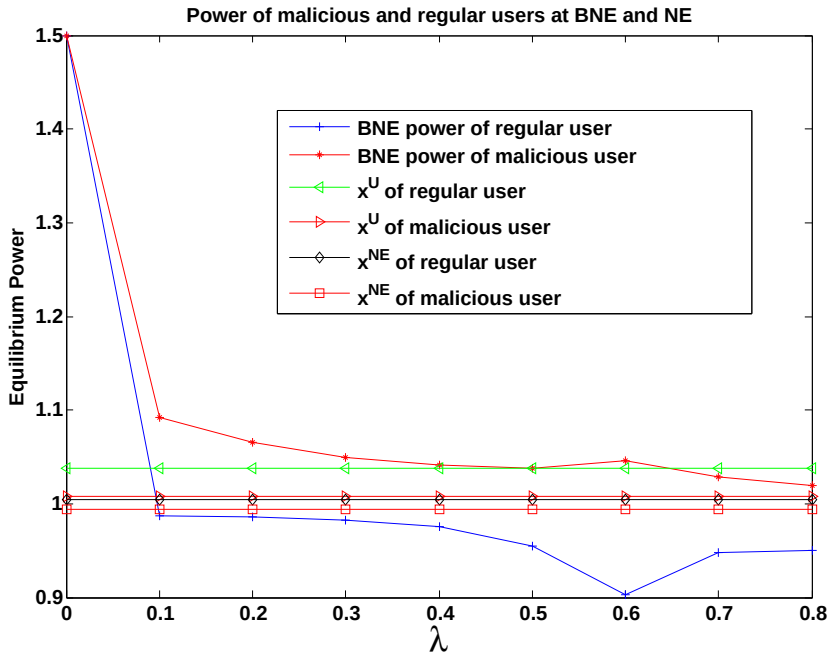

Figure: BNE powers in pricing mechanism.

Summary

- Wireless network with an arbitrary number of malicious users is considered. It is observed that the BNE points of the pricing game is not unique and are obtained numerically.
- The user misbehavior is detected by learning anomalies in the utilities.
- The malicious users are priced higher using the probabilistic statistic from the detection.

Thank you!

References I

- A. K. Chorppath, T. Alpcan, and H. Boche, "Games and Mechanisms for Networked Systems: Incentives and Algorithms", in "Mechanisms and Games for Dynamic Spectrum Allocation", Cambridge University Press, 2013, Editors: T. Alpcan, H. Boche, M. Honig, H. V. Poor.
- 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, T. Alpcan, and H. Boche, "Bayesian Mechanisms for Wireless Network Security", IEEE International Conference on Communications (ICC), June 2014, Sydney, Australia.
- F. Shen, E. A. Jorswieck, A. K.Chorppath and H. Boche,"Pricing for Distributed Resource Allocation in MAC without SIC under QoS Requirements with Malicious Users ", WNC, IEEE Wiopt, May, 2014.