Bayesian Mechanisms for Wireless Network Security

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

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

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

***Abstract*—Strategic users in a wireless network cannot be assumed to follow the network algorithms blindly. Moreover, some of these users could be controlled by powerful Botnets, which aim to use their knowledge about network algorithms to maliciously gain more resources and also to create interference to other users. We consider a scenario; in which a mechanism designer and legitimate users together, in a wireless network, gather probabilistic information about the presence of malicious users and modify their actions accordingly. The probabilistic information is gathered by observing the network over a long time period. We study Bayesian mechanisms, both pricing schemes and auctions, and obtain the Nash Equilibrium (NE) points of the underlying Bayesian games. The NE points provide conditions indicating when it is better for users to to hide or reveal their nature(types). The prices and allocations in the mechanisms are later modified using the Bayesian information about the type of the users. The numerical studies show the NE points and illustrate the results.**

I. Introduction

There has been a shift in focus in wireless network research over the past few years, on decision making and incentives in the presence of malicious users, who create inefficiencies in allocation of network resources or even disrupt them ([1], [2]). Wireless devices are getting highly capable, but at the same time prone more to security threats from increasingly sophisticated attacks.

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 botnets by a malicious agent(botmaster). Botnets [3] 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 network bandwidth and resources of the bots, that way deny the legitimate access to the resources. The high interconnectivity of the wireless network with the Internet makes these networks highly vulnerable to botnet attacks. In [4], 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, they have demonstrated in [4], 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. A related case where femtocells are compromised as bots is analyzed in [5]. In [6], a Bayesian detection using the Domain Name System (DNS) traffic similarity to the known bots belonging to the same botnet is studied.

In this paper, we model botnets, in which compromised devices, known as bots, act like regular users accepting the mechanism rules determined by the network (designer). By accepting the price and allocation rules, they avoid immediate detection and continue having access to resources such as transmission power and rate. The legitimate (regular) users and the designer know only the probability with which a mobile device could be a bot or not and we 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.

We study in this paper the conditions, under which malicious users decide to hide or reveal their identity. The boundary conditions are based on the system parameters. We analyze Bayesian mechanisms [7] which comprise a designer who designs allocation and prices based on information which is expressed as a probabilistic distribution over the types of the users. The impact of the malicious behavior is quantified within a Bayesian framework and malicious behavior resistant mechanisms are designed. In the mechanisms we consider, the users are uncertain about the nature of other users, i.e. whether others are regular users or botnets (jammers). We extend the work in [8] to an incomplete information case where the malicious users are countered without explicit detection or learning. We assume only that the designer knows the probability of malicious users' existence and he counters them by updating the prices using the probabilistic information.

In [9], Bayesian jamming games are considered and the Nash Equilibrium (NE) points for different jamming scenarios are obtained. Unlike the work in [9], we consider pricing mechanisms and auctions [10] in the presence of malicious users and also modify them 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 regular users. We also use a different model of the malicious behavior in this paper compared to the one in [9]. The new model is proposed in our prior work in [8], where the malicious user is interested in his own utility and

The work by Anil Kumar Chorppath and Holger Boche is supported by the COIN project by German National Science Foundation (DFG) BO 1734/24-1.

978-1-4799-2003-7/14/$31.00 ©2014 IEEE

has a degree of maliciousness. Our aim is to obtain prices in a Kelly-type mechanism [11], for interference coupled networks in the presence of malicious users. In the scenario considered, botnets or jammers hide among the crowd of regular users accepting the prices and allocations, but they overuse resources for their purpose and harm others this way.

II. Model

The model and assumptions which we present in this section are based on our earlier paper, [8], and is partially repeated here for completeness. At the center of the mechanism design model is the *designer* $\mathcal{D}$ who influences N *users*, denoted by the set $\mathcal{A}$. The N users are participating in a **strategic (noncooperative) game** [12]. These users are autonomous and rational decision makers, who share and compete for limited resources of the network under the constraints particular to the network. Let us define an N-player strategic game, $\mathcal{G}$, where each player $i \in \mathcal{A}$ has a respective **decision variable** x_i such that

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

where $\mathcal{X}$ 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 variable of users other than i^{th} user and $\mathcal{X}_{-i}$ is the respective decision space. The strategy space $\mathcal{X} \subset \mathbb{R}^N$. We make the following assumption which is necessary for the existence of NE.

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

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

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

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, nondecreasing and strictly concave in x_i.

The modified utility function can be obtained by a convex combination of user utility functions

$$U_i^m(\mathbf{x}) = U_i(\mathbf{x}) + \theta_i \sum_{k \neq i} U_k(\mathbf{x}), \tag{1}$$

where θ_i is the parameter between -1 and 1 which captures the range of behavior of a user, from malicious to altruistic. We assume that malicious users do not gain anything by interfering each other. For a malicious user, the variable θ is negative and is called *degree of maliciousness*.

Let user j be a jammer with a probability of ψ_j. The Jammer spends an energy B^m for transmission per unit of power which is usually different compared to the energy B^s spent by the regular users.

The designer $\mathcal{D}$ devises a **mechanism** $\mathcal{M}$, which is represented by the mapping $M : \mathcal{X} \to \mathbb{R}^N$, by introducing incentives in the form of *allocation rules and prices* to users. Let $C_i(\mathbf{x})$ is the total payment by the i^{th} user to the mechanism and $Q_i(\mathbf{x})$ be the received power allocation to the i^{th} user.

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

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

where L is the processing gain and σ^2 denotes noise power.

The individual transmission power of the users will be, $\frac{Q_i}{h_i}$, where, h_i $\forall i$, are the channel gains. The utility functions we consider are functions of SINR, i.e., $U_i(\gamma_i(Q_i, Q_{-i}))$. To quantify the effect of the malicious behavior a metric, PoM, was proposed in [8] which is defined as,

Definition II.4. *The metric Price of Malice(PoM) of a mechanism $\mathcal{M}$ is defined as:*

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

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

III. Bayesian Pricing Mechanisms

In pricing mechanisms, the users choose their allocation as their strategy or action. Pricing mechanisms [10] do not have explicit allocation rule, i.e., $x_i = Q_i$, $\forall i$. The pricing mechanisms are more appropriate for modeling distributed systems where we cannot expect a central authority to allocate resource to the users. Let $\mathbf{x}$ be the receiver power vector and $\mathbf{P}$ be the price vector per received power such that $C_i = P_i x_i$.

The prices which are proposed in [13] for social optimum point in the N user case, modified with the energy cost $\mathbf{B}$, are obtained by the matrix equation,

$$A \cdot \mathbf{P} = D \cdot \mathbf{L} - \mathbf{B1}, \tag{3}$$

where

$$A := \begin{pmatrix} 1 & -\gamma_2 & \cdots & -\gamma_N \\ -\gamma_1 & 1 & \cdots & -\gamma_N \\ \vdots & & \ddots & \vdots \\ -\gamma_1 & -\gamma_2 & \cdots & 1 \end{pmatrix}, \tag{4}$$

$$D := \begin{pmatrix} \frac{1}{h_1} & 0 & \cdots & 0 & \frac{1}{h_1} \\ 0 & \frac{1}{h_2} & \cdots & 0 & \frac{1}{h_2} \\ \vdots & & \ddots & \vdots & \\ 0 & 0 & \cdots & \frac{1}{h_N} & \frac{1}{h_N} \end{pmatrix}, \tag{5}$$

$\mathbf{L} = [\lambda_1, \ldots, \lambda_N, \mu]^T$, $\mathbf{1} = [1, \ldots, 1]^T$ and $\lambda_1, \ldots, \lambda_N$ and μ are the Lagrange multipliers for the following designer prob-

lem. The designer solves the global optimization problem,

$$\max_{\mathbf{x}} \sum_i U_i(\gamma_i(\mathbf{x})), \text{ s. t.} \sum_i \frac{x_i}{h_i} \leq X_t \ , x_i \geq 0 \forall i. \quad (6)$$

The SINR values $\gamma_1, \ldots, \gamma_N$ are measured at the receiver and are side information which depends on the utility functions of the users.

For the two users case the prices for User 1 turn out to be

$$P_1 = \frac{1}{1-\gamma_1\gamma_2}\left(B^s\gamma_1\gamma_2 + \frac{\gamma_2(\lambda_1+\mu)}{h_1} + \frac{(\lambda_2+\mu)}{h_2}\right), \quad (7)$$

and similarly for User 2.

A. Case of Only 1 User of Unknown Type

Let $N-1$ users have regular selfish behavior and have only probabilistic information about user j whose nature is unknown. Let x_i be the received power at the base station for regular user i, who has the utility function

$$U_i(\mathbf{x}) = \log\left(\gamma_i(\mathbf{x})\right) = \log\left(\frac{x_i}{\frac{1}{L}\sum_{j\neq i} x_j + \sigma^2}\right). \quad (8)$$

The cost function of all regular users will be,

$$\begin{aligned} J_i(\mathbf{x}) = P_i x_i \quad &+ \quad B^s\frac{x_i}{h_i} - \psi_j \log\left(\gamma_i(\mathbf{x}_{-j}, x_j^m)\right) \\ &- \quad (1-\psi_j)\log\left(\gamma_i(\mathbf{x}_{-j}, x_j^s)\right), \ \forall i \end{aligned} \quad (9)$$

where x_j^s and x_j^m are the powers of user j when it is regular and jammer respectively. Note that the price is on the received power but the energy cost is on the transmitted power. Regular users minimize J_i subject to $x_i \geq 0, \ \forall i$. The cost function of User j if it is regular is,

$$J_j^s(\mathbf{x}) = P_j x_j^s + B^s\frac{x_j^s}{h_j} - \log\left(\gamma_j(x_j^s, \mathbf{x}_{-j})\right), \quad (10)$$

The cost function of user j if it is malicious is,

$$\begin{aligned} J_j^m(\mathbf{x}) \quad &= \quad P_j x_j^m + B^m\frac{x_j^m}{h_j} - \log\left(\gamma_j(x_j^m, \mathbf{x}_{-j})\right) \\ &- \quad \theta_i \sum_{k\neq i} \log\left(\gamma_i(\mathbf{x}_{-j}, x_j^m)\right) \end{aligned} \quad (11)$$

User j minimize J_j^s or J_j^m depending on the type, subject to $x_j^m, x_j^s \geq 0$.

The NE points can be obtained from the BR and results are given below for $N = 2$.

Proposition III.1. *The power strategies of the Regular user and the User of Unknown Type at the Bayesian NE point for a game between two users of logarithmic utility function given in (8) are given by,*

$$x_2^s = \frac{1}{P_2 + \frac{B^s}{h_2}}, \quad (12)$$

$$x_1 = \frac{1}{P_1 + \frac{B^s}{h_1}}, \quad (13)$$

and x_2^m given by solution of

$$x_2^{m2} + x_2^m\left(\frac{L\sigma^2}{P_2 + \frac{B^m}{h_2}} - (1-\theta_2)\right) - L\sigma^2 = 0, \quad (14)$$

where the prices P_1 and P_2 follow from (7).

Proof: The KKT conditions for the BR of the regular user are given by,

$$P_2 + \frac{B^s}{h_2} - x_2^s + \frac{\lambda^s}{h_2} = 0 \text{ and } x_2^s\lambda^s = 0 \quad (15)$$

which gives (12) and is same for User 1. In a similar way, (14) can be obtained from the malicious user cost function in (11). ■

We could observe that the uncertainty on the nature of User 2 does not affect the strategy of the regular User 1. This is due to the particular choice of the logarithmic utility function. Therefore, it does not make any difference if the regular and user of unknown nature hides or reveals its utility.

Let us consider the case of linear SINR utility function

$$U_i(\gamma_i) = \gamma_i(\mathbf{x}). \quad (16)$$

For this case the Bayesian NE (BNE) is given below for two users case.

Proposition III.2. *The power strategies of the Regular user and the User of Unknown Type at the BNE point for a game between two users of linear utility function given in (16) are given by,*

$$x_1 = \left[\frac{1}{h_1}\left(\frac{h_2}{P_1 + B^s} - \sigma^2\right)\right]^+ \quad (17)$$

$$x_2^m = \left[\sqrt{\frac{-\theta_2 x_1}{P_2 + \frac{B^m}{h_2} - \frac{1}{x_1+\sigma^2}}} - \frac{\sigma^2}{h_2}\right]^+ \quad (18)$$

$$x_2^s = \frac{1}{h_2}\left[\frac{h_1(1-\psi_2)}{P_2 + B^s - \frac{\psi_2 h1}{h_2 x_2^m + \sigma^2}} - \sigma^2\right]^+ \quad (19)$$

where the prices P_1 and P_2 follow from (7).

The proof follows similar to the proof of Proposition III.1. Assume that the User 2 is inherently regular. Then the power it would use if it reveals its nature is

$$x_2 = \left[\frac{1}{h_2}\left(\frac{h_1}{P_2 + B^s} - \sigma^2\right)\right]^+.$$

The condition under which it is profitable for User 2 to hide its nature is given by

$$\frac{h_1}{P_2 + B^s} > h_2 x_2^m + \sigma^2, \quad (20)$$

so that x_2^s is greater than x_2. We could see that when User

2 sees that the opponent (User 1) has high channel gain, h_1, and there is low price of transmission P_2, it is good for to him to hide his nature. Therefore, a higher price for all the users will force all of them further to reveal their type. Similarly, we could also obtain the condition for which an inherently malicious user will hide his type from (18) but which depends on θ_2 but not on ψ_2.

Consider the case where, the designer has only probabilistic information about User 2 and needs to modify the prices according to this information. Let us analyze how the designer can modify the pricing using this limited information. The designer adds the utility of the User 2 only if that user is regular. Let ψ_2' be the probability belief with which another user is a jammer for the designer assuming it has the better level of information than a regular user. The new global objective of the designer is,

$$U_1 + (1-\psi_2')U_2. \tag{21}$$

and it should update the prices according to this new objective.

Proposition III.3. *For the two users case with designer having only Bayesian information, the prices for User 2 of unknown type will be,*

$$P_2 = \frac{1}{(1-\psi_2')(1-\gamma_1\gamma_2)}\left(B^s\gamma_1\gamma_2 + \frac{\gamma_2(\lambda_1+\mu)}{h_1} + \frac{\lambda_2+\mu}{h_2}\right) \tag{22}$$

and for User 1 it will be same as in (7).

Proof: The prices are obtained as the same way of alignment of user and designer objective through prices as in [13] with the modified designer objective in (21). ∎

Therefore, we could see that the user with uncertain user type receives higher price and this motivate the user to reveal its type. These are the prices in a Kelly-type mechanism [11] for interference coupled networks in the presence of malicious users.

B. Case 2: All Users of Unknown User Type

We consider now the case where the users have only probabilistic information about the nature of other users. The designer also has only probabilistic information about the type of all the users. Let ψ_j and ψ_j^m be the probability belief with which another user is a jammer for regular and malicious nodes. If a user is regular, it receives the price P_s and if it is malicious P_m. Each node assume that other nodes of same type choose the same strategy. The following proposition gives the BNE power strategies of the regular user and the malicious user with logarithmic utilities.

Proposition III.4. *In the case of two users, the power strategy of the malicious user at the BNE point for logarithmic utility functions when both users have unknown user type are given by,*

$$x_m = \left[\frac{-\theta_j(1-\psi_j^m)}{P_m + \frac{B^m}{h^m}\left(\theta_j(1-\psi_j^m) - \psi_j^m\right)} - \sigma^2\right]^+ \tag{23}$$

and of the regular user is the solution of

$$x_s^2(P_s + B^s h^s) + x_s\left(\sigma^2\left(P_s + B^s h^s\right) - \psi_j\right) - \sigma^2 = 0 \tag{24}$$

Proof:

In the two users case, the cost function of the user s if it is regular is given by,

$$\begin{aligned} J^s = P_s x_s &+ B^s\frac{x_s}{h_s} - (1-\psi_j)U_{ss}(x_s, x_s) \\ &- \psi_j U_{sm}(x_s, x_m) \end{aligned} \tag{25}$$

where U_{ss} is the utility of selfish user when the other user is also selfish and U_{sm} is the utility of selfish user when the other user is malicious. For log utility given in (8),

$$\begin{aligned} J^s = P_s x_s &+ B^s\frac{x_s}{h_s} - (1-\psi_j)\log(\gamma_s(x_s, x_s)) \\ &- \psi_j \log(\gamma_s(x_s, x_m)). \end{aligned} \tag{26}$$

The cost function of the malicious node m is given by,

$$\begin{aligned} J^m = P_m x_m &+ B^m\frac{x_m}{h_m} + (1-\psi_j^m)\theta_j U_{ms}(x_m, x_s) \\ &- \psi_j^m U_{mm}(x_m, x_m) \end{aligned} \tag{27}$$

and for log utility

$$\begin{aligned} J^m = P_m x_m &+ (1-\psi_j^m)\theta_j\left(\log(\gamma_s(x_m, x_s)) + B^m\frac{x_m}{h_m}\right) \\ &+ \psi_j^m B^m\frac{x_m}{h_m}. \end{aligned} \tag{28}$$

From the KKT conditions of the BR using these cost functions, we could obtain the BNE point. ∎

When there are more number of users in the network, the power strategies will be similar but involve combination.

When both users are of unknown type, the global objective of the designer changes as,

$$\max_x \sum_i (1-\psi_i')U_i(\gamma_i(\mathbf{x})) \text{ s. t. } \sum_i \frac{x_i}{h_i} \le X_t \ , x_i \ge 0 \forall i. \tag{29}$$

where ψ_i' is the belief that a user is malicious. For the 2 users case with designer having only Bayesian information, the prices for all the users will be, given by (22). Therefore, we could see that the users receive higher price when there is a higher probability of having malicious users in the network.

We could obtain the PoM using these NE points according to the Definition II.4. In the two users case, this is as follows

$$PoM(\mathcal{M}) := \frac{U_1(\gamma_1(x_1, x_2^s)) - U_1(\gamma_1(x_s, x_m))}{U_1(\gamma_1(x_1, x_2^s))},$$

where x_2^s by (12),x_1 is given by (13) , x_s by (23) and x_m by (24).

IV. Auctions with Malicious Users

We now consider auction mechanisms in which the designer (base station) makes centralized decisions on the power level and price for all users, which is the case in the practical wireless networks and standards now. In auctions, power allocations $\mathbf{Q}$ and prices $\mathbf{C}$ are centrally calculated by a designer and the users respond to them with the bids or

strategies $\mathbf{x}$. We analyze how the uncertainty about the type of users change the strategizing in the auction mechanisms.

In [8] an efficient mechanism is proposed in which the allocation and pricing for social efficient point are,

$$Q_i(\mathbf{x}) = \frac{x_i}{\sum_j x_j + \omega} X_t, \tag{30}$$

$$C_i(\mathbf{x}) = x_i \sum_{j \neq i} x_j + \omega, \tag{31}$$

where ω is the reserve price.

We analyze the equilibrium points which arise when the users take best response to the pricing and allocation set by the base station. For the allocation given in (30), taking $\omega = 0$, the SINR at NE point x^* is

$$\gamma_i(\mathbf{x}^*) = \frac{x_i^* X_t L}{\sum_{j \neq i} x_j^*(X_t + L\sigma^2) + x_i L\sigma^2}. \tag{32}$$

Consider the two users case with one of the user of uncertain type and log utility for all the users. The cost function of the regular User 1 anticipating that it will receive an SINR given in (32) is

$$\begin{aligned} J_1 &= B^s \frac{x_1}{h_1} + \psi_2 (x_1 x_2^m - \log(\frac{x_1 X_t L}{x_2^m(X_t + \sigma^2 L) + x_1 \sigma^2 L})) \\ &+ (1 - \psi_2)(x_1 x_2^s - \log\left(\frac{x_1 X_t L}{x_2^s(X_t + \sigma^2 L) + x_1 \sigma^2 L}\right) \end{aligned} \tag{33}$$

where x_2^s and x_2^m are the powers of User 2 when it is regular and jammer respectively. User 1 minimize J_1 subject to $x_1 \geq 0$. The cost function of user 2 if it is regular is,

$$J_2^s(x_1, x_2^s) = x_1 x_2^s + B^s \frac{x_2^s}{h_2} - \log\left(\frac{x_2^s X_t L}{x_1(X_t + \sigma^2 L) + x_2^s \sigma^2 L}\right). \tag{34}$$

The cost function of user 2 if it is malicious is,

$$\begin{aligned} J_2^m &= x_1 x_2^m + B^s \frac{x_2^m}{h_2} - \log\left(\frac{x_2^m X_t L}{x_1(X_t + \sigma^2 L) + x_2^m \sigma^2 L}\right) \\ &- \theta_i \log\left(\frac{x_1 X_t L}{x_2^m(X_t + \sigma^2 L) + x_1 \sigma^2 L}\right). \end{aligned} \tag{35}$$

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 V.

The designer observing that there is a possibility that some of the users could be malicious (botnet), modifies the allocation and pricing rule accordingly. If a user j is expected to be malicious by designer with probability ψ_j', the allocation of that user should be modified to,

$$Q_j = (1 - \psi_j') \frac{x_j}{\sum_k x_k + \omega} X_t, \tag{36}$$

and the pricing as

$$C_j = x_j \sum_{k \neq j} x_k + \omega - \psi_j'(N-1) t X_t \log\left(1 + \frac{x_j}{\sum_{k \neq j} x_k}\right). \tag{37}$$

The pricing is a Bayesian version of the *differentiated pricing* given in Section VIII of [8] and it is proven in the line of proof given in [8], that this will compel the bot to realize that it has been used by a botnet since it obtained disproportional higher price than its power usage.

V. Simulation

We numerically illustrate the results summarized in the Propositions presented in the previous sections.

First, we simulate auction given in Section IV with $N = 20$ users out of which only one user is of uncertain type and others are regular users. We assume that all regular users have same channel gains. The NE points are obtained by solving the BR obtained from the cost functions given in equations (33), (34) and (35), but for N users. The system parameters used are $\psi = 0.5, \omega = 0, \sigma = 0.1$, $X_t = 10$ and $L = 0.01$. In Figure 1, the NE points are plotted when the User j who is a malicious user hides and reveals its nature, as a function of θ_j. We could see that when $\theta_j > -0.42$, its better for the User j to hide its type. The User j should hide its type when there is higher ambiguity about its nature, i.e., when θ_j is close to 0 and should not hide when it is highly malicious, i.e., when θ_j is closer to -1. It is also observed that for the given system parameters, it is better for User j to reveal its type if it is inherently regular.

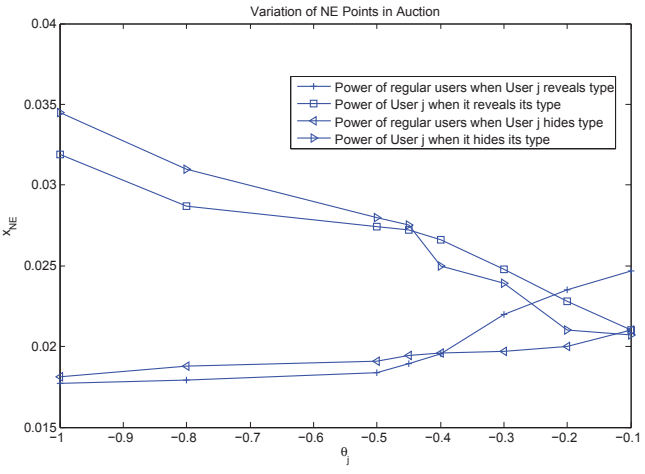

Fig. 1. The variation of NE points when the User j who is a malicious user hides and reveals its nature, as a function of degree of maliciousness θ_j.

Next we plot the NE points in pricing when both users have unknown type, as a function of probability of malicious ψ_2 and the resulting PoM in Figure 2. We observe that the regular user increases its power, as the probability of malicious user (ψ_2) increases, since it takes into account the impact of the maliciousness more in its utility function. In other words, the regular user is more anticipating the malicious effect when it chooses the power. The PoM is observed to be negative for this case since the regular user has higher utility when the nature of the other user is unknown. This paradoxical result is usually referred to as *windfall of malice* [9].

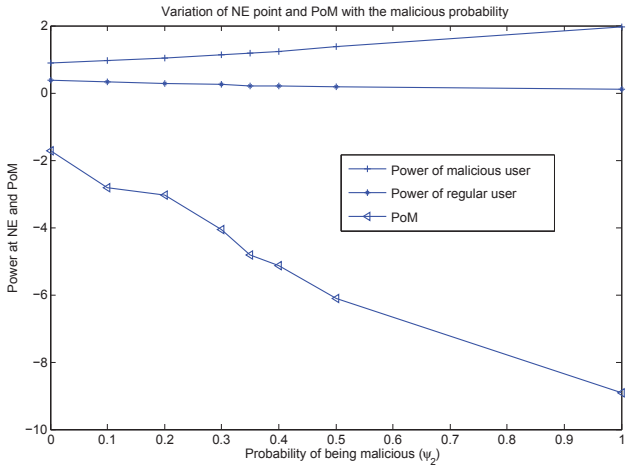

Fig. 2. The variation of NE points when both users have unknown type, as a function of probability of malicious ψ_2 and the resulting PoM.

VI. Conclusion

We have investigated situations where a mechanism designer and legitimate users in a wireless network gather probabilistic information about the presence of malicious users(bots) by observing the network over a long time period and modify their actions. We have studied Bayesian mechanisms, both pricing schemes and auctions, and obtained the Nash Equilibrium (NE) points of the underlying Bayesian games. The effect of malicious actions is quantified using the PoM parameter. We have obtained conditions under which it is better for the regular or malicious users to reveal their nature or face increasing costs. The conditions were obtained which suggests the users when to hide and reveal the type, depending on the wireless network physical layer parameters. We have also devised centralized methods to counter wireless network threats from botnets and jammers using prices and resource allocation algorithms. We have observed a case of *windfall of malice* through numerical results. The possible extension is to a setting in which users have QoS requirements. Another one is the analysis of the case where Femto base stations are used as bots as in [5].

References

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

[2] S. Bhattacharya, A. Khanafer, and T. Başar, "Power allocation in team jamming games in wireless ad hoc networks," in *Proceedings of the 5th International ICST Conference on Performance Evaluation Methodologies and Tools*, ser. VALUETOOLS '11. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2011, pp. 515–524.

[3] 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)*, 2008, pp. 967–972.

[4] 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*, ser. CCS09, 2009.

[5] N. Golde, K. Redon, and R. Borgaonkar, "Weaponizing femtocells: The effect of rogue devices on mobile telecommunications," in *19th Annual Network and Distributed System Security Symposium, (NDSS 2012)*, San Diego, 2012.

[6] R. Villamarn-Salomn and J. C. Brustoloni, "Bayesian bot detection based on dns traffic similarity," in *ACM Symposium on Applied Computing, SAC09*, Honolulu, Hawaii, 2009.

[7] D. Garg, Y. Narahari, and S. Gujar, "Foundations of Mechanism Design: A Tutorial Part 1 - Key Concepts and Classical Results," *Sadhana*, vol. 33, no. 3, pp. 83–130, April 2008.

[8] A. K. Chorppath, T. Alpcan, and H.Boche, "Adversarial behavior in network games," *Dynamic Games and Applications*, June 2013.

[9] Y. Sagduyu, R. Berry, and A. Ephremides, "MAC games for distributed wireless network security with incomplete information of selfish and malicious user types," in *Game Theory for Networks, 2009. GameNets '09. International Conference on*, 2009, pp. 130–139.

[10] A. K. Chorppath, T. Alpcan, and H. Boche, *Mechanisms and Games for Dynamic Spectrum Allocation*. Cambridge University Press, 2013, ch. Games and Mechanisms for Networked Systems: Incentives and Algorithms.

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

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

[13] 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.