Resource Allocation in Fading Multiple Access Wiretap Channel via Game Theoretic Learning

Shahid Mehraj Shah, Krishna Chaitanya A and Vinod Sharma
Department of Electrical Communication Engineering,
Indian Institute of Science, Bangalore, India
Email: {shahid, akc, vinod}@ece.iisc.ernet.in

***Abstract*—In this paper we consider a K-user fading multiple access wiretap channel, where each user wants to transmit a message confidentially. There is a passive eavesdropper (Eve) at the receiving end. We are interested in allocating rates and powers to the users fairly and reliably without the eavesdropper being able to decode the message. Initially we assume that each user knows only its own channel gain to the receiver and to the eavesdropper. When any user transmits a message, the receiver send an ACK if the message is decoded correctly and confidentially, else it sends a NACK. We use *Multiplicative Weight* no-regret algorithm to obtain a coarse correlated equilibrium. Next we maximize the weighted sum of utility of all the users and obtain Pareto optimal points. Since not all Pareto points are fair, we also obtain Nash Bargaining (NB) solutions which ensure certain fairness to all the users. In the next part of the paper we make more realistic assumption that each user knows only its own channel gain, and is ignorant of the channel gain to Eve (only its distribution is known). We use secrecy outage as the metric at the receiver to decide weather the message is correctly decoded or not. We obtain a coarse correlated equilibrium, a Pareto point and a Nash bargaining solution.**

***Index Terms*—Physical layer security, multiple access channel, fading channel, no-regret algorithm, game theory, Nash bargaining solution, Pareto point.**

I. Introduction

Secure uplink and downlink communication is gaining importance as more and more vital information is transmitted over the wireless devices. A fading multiple access channel with a wiretapper (F-MAC-WT) is a basic model for a secure-uplink communication system wherein several users want to transmit their messages confidentially to a legitimate receiver. Also there is an adversary (Eve) present at the receiving end, who is passively listening and trying to decode the messages.

Multiple access wiretap channel (MAC-WT) is well studied in literature. One of the early works is reported in [1] where only one user has confidential messages to be transmitted. The authors have obtained upper bounds on the secrecy-rate regions. In [2] the authors consider a more general setup wherein they consider a discrete memoryless multiple access channel where the transmitting users receive the noisy version of each others' conversation, and they do not trust each other. In that scenario the authors have studied an achievable secrecy rate region and some outer bounds. In some special cases secrecy capacity region is obtained. Multiple access wiretap channel with feedback has been studied in [3]. An achievable region of a Gaussian multiple access wiretap channel (G-MAC-WT) was obtained in [4], (the secrecy capacity region is still an open problem).

In all the previous works, weak secrecy criterion is used. A strong secrecy based achievable rate region for a MAC-WT is reported in [5]. In [6] the authors find secure degrees of freedom for a MAC-WT. More recently in [7] the authors have studied compound MAC-WT and have characterized inner and outer bounds of the secrecy capacity region. In [8] the authors have studied a fading MAC-WT with full CSI of Eve and also when each user knows the channel state of all the users to the receiver, but is ignorant of the instantaneous value of channel state to the eavesdropper (only its distribution is known). But knowing other users' channel gains to the legitimate receiver may also not be practical: it needs a lot of signalling overhead and feedback information. Hence in this paper we present a game-theoretic solution to the resource allocation scheme under the hypothesis that each user only knows its own channel gain and is completely ignorant of other users' channels (not even the distributions).

We first consider the case where each user knows its own channel gain to the receiver and the eavesdropper. The receiver knows channel gains of all the users. When any user transmits a message, the receiver sends an ACK (acknowledgement) if the rate at which message is transmitted is in secrecy rate region, else the receiver sends a NACK (negative acknowledgement). The utility at the transmitting end is defined based on the reception of an ACK/NACK. We pose this problem as a stochastic game and use no-regret based multiplicative weight algorithm ([9], [10]) to obtain a coarse correlated equilibrium (CCE). Next we assume that each user can also track ACK/NACK of other users, and propose a Pareto optimal (PP) policy which is socially optimal. We also obtain a Nash bargaining solution (NBS) in this setup.

Since it is not practical to assume instantaneous channel gain of the eavesdropper to be known at the transmitter and the receiver, we next consider the case where the receiver only knows the distribution of the Eve's channel gains. The receiver calculates secrecy-outage probability and sends an ACK/NACK based on that. We again obtain a CCE, PP and a NBS. Finally we compare the sum-rates obtained via all these algorithms to the global CSI case and also with the sum-rate obtained in [8].

Without security constraints, game-theoretic learning algorithms have been used to study power allocation in interference

channels in [11]. Game theoretic formulation of a fading MAC has been studied in [12], where the authors assume that each user knows the CSI of the other users and propose a distributed algorithm to allocate power to each user. The authors prove that the Nash equilibrium in the waterfilling game is a sum-rate point. By using Stackelberg formulation, the authors also achieved other points of the capacity region of a fading MAC. The assumption that each user knows all other users' channel gains was relaxed in [13], and it was assumed that each user only knows the distribution of the channel gains of the other users. The authors prove the existence of a Bayesian equilibrium and maximize the sum-rate of the users.

The rest of the paper is organized as follows. In Section II we describe the channel model and formulate the problem. In Section III we use Multiplicative Weight Algorithm to obtain a CCE. In Section IV we obtain Pareto optimal points. In Section V we a consider fading-MAC-WT (F-MAC-WT) when the CSI of Eve is not available at the transmitters (only its distribution is known) and obtain a CCE, a NBS, and a PP. In Section VI we compare the various schemes on an example. Finally, in Section VII we conclude the paper.

II. Channel Model and Problem Formulation

A time slotted F-MAC-WT channel is considered with K-users who have messages to be transmitted confidentially to a legitimate receiver (Bob), while a passive eavesdropper (Eve) is listening to the conversation and trying to decode. Let $\{\widetilde{H}_i(t)\}$ be the channel gain process from user i to the receiver and $\{\widetilde{G}_i(t)\}$ the channel gain process from user i to Eve. At time t user i transmits $X_i(t)$ and Bob receives $Y(t)$ and Eve receives $Z(t)$ where,

$$Y(t) = \sum_{i=1}^{K} \widetilde{H}_i(t) X_i(t) + \eta_b(t), \tag{1}$$

$$Z(t) = \sum_{i=1}^{K} \widetilde{G}_i(t) X_i(t) + \eta_e(t), \tag{2}$$

and $\eta_b(t), \eta_e(t)$ are white Gaussian noise, both with distribution $\mathcal{N}(0,1)$ and independent of each other. We define $H_i(t) \triangleq |\widetilde{H}_i(t)|^2$ and $G_i(t) \triangleq |\widetilde{G}_i(t)|^2$. These are assumed discrete valued, in the sets $\mathcal{H}_i \triangleq \{h_i^{(1)}, \ldots, h_i^{(M)}\}$ and $\mathcal{G}_i \triangleq \{g_i^{(1)}, \ldots, g_i^{(M)}\}$. Also $\{H_i(t), t \geq 0\}$ are independent and identically distributed (iid) sequences with distributions $\{\alpha_i^{(1)}, \ldots, \alpha_i^{(M)}\}$ and $\{G_i(t), t \geq 0\}$ are iid with distributions $\{\beta_i^{(1)}, \ldots, \beta_i^{(M)}\}$. To transmit any codeword, user i can choose any power level from the set $\mathcal{P}_i \triangleq \{P_i^{(1)}, \ldots, P_i^{(M)}\}$. Also, user i has average power constraint $\overline{P}_i$.

User i transmits at a fixed rate r_i via wiretap coding, as in [4]. If the receiver successfully decodes from a user, it sends an ACK to that particular user. Otherwise it sends a NACK. We assume that the NACK, ACK are transmitted at low rates with robust codes so that these can be received with negligible error at the intended transmitter.

Each user i is assumed to know its own channel gains $H_i(t)$ and $G_i(t)$ at time t. Since the legitimate receiver can estimate the channel gain of all the users (either by receiving known pilots or by using initial data received), the receiver can use successive decoding strategy to decode all the users.

Let $\pi(i)$ be the user which has the i^{th} highest channel gain (in case of a tie we arbitrarily order them). The decoder first decodes the user $\pi(1)$ with the best channel gain first, taking the transmissions from the other users as noise. Then it removes it from the received signal $Y(t)$ and decodes the next best user, taking the other users as noise and so on.

The following notation will be used in the rest of the paper:

$$C_b\left(P_{\pi(i)}, P_{-\pi(i)}, H_{\pi(i)}, G_{\pi(i)}\right) \triangleq \frac{1}{2}\log\left(1 + \frac{H_{\pi(i)}P_{\pi(i)}(H_{\pi(i)}, G_{\pi(i)})}{1 + \sum_{j=i+1}^{K} H_{\pi(j)}P_{\pi(j)}(H_{\pi(j)}, G_{\pi(j)})}\right), \tag{3}$$

$$C_e\left(P_{\pi(i)}, P_{-\pi(i)}, H_{\pi(i)}, G_{\pi(i)}\right) \triangleq \frac{1}{2}\log\left(1 + \frac{G_{\pi(i)}P_{\pi(i)}(H_{\pi(i)}, G_{\pi(i)})}{1 + \sum_{j\neq i}^{K} G_{\pi(j)}P_{\pi(j)}(H_{\pi(j)}, G_{\pi(j)})}\right). \tag{4}$$

Then the receiver will send an ACK to transmitting user $\pi(i)$ if

$$r_{\pi(i)} \leq \left(C_b(P_{\pi(i)}, h_{\pi(i)}, g_{\pi(i)}) - C_e(P_{\pi(i)}, h_{\pi(i)}, g_{\pi(i)})\right)^+ \tag{5}$$

The above constraint follows from the achievable secrecy-rate region of Gaussian MAC-WT as discussed in [4].

Each user i takes action (allocating power) $P_i^{(j)}$ when its channel gains are $H_i^{(j)}$ and $G_i^{(j)}$ to transmit at its rate. We define feasible action space for user i as

$$\mathcal{P}_i = \Big\{\mathbf{P}_i = (P_i^{(1)}, \ldots, P_i^{(M)}) : P_i^{(k)} \in \{p_i^{(1)}, \ldots, p_i^{(M)}\}, \sum_{j=1}^{M} \alpha_i(j)\beta_i^{(j)} P_i^{(j)} \leq \overline{P}_i\Big\}. \tag{6}$$

We define $|\mathcal{P}_i| \triangleq M_i$ (where $|A|$ denotes the cardinality of set A) and index the elements of set $\mathcal{P}_i$ as $\{1, \ldots, M_i\}$. Let a_i denote a feasible power policy of user i, i.e., a_i takes a value from $\mathcal{P}_i$, and $a_i(h_i, g_i)$ is the power level used by user i when its channel gains are h_i, g_i under policy a_i. The action space of the K users is denoted as

$$\mathcal{P} = \bigotimes_{i=1}^{K} \mathcal{P}_i, \tag{7}$$

and the action space of users, other than user i is

$$\mathcal{P}_{-i} = \bigotimes_{j=1, j\neq i}^{K} \mathcal{P}_j, \tag{8}$$

where $\bigotimes_{i=1}^{N} A_i = A_1 \times A_2 \ldots \times A_N$. The action profile of all the users is denoted as $a = (a_1, \ldots, a_K)$. A probability distribution $\psi(i)$ on $\mathcal{P}_i$ is called a mixed strategy of user i. When a certain action is chosen with probability one, it is

called a *pure strategy*. The objective of each transmitter is to maximize its probability of successful transmission. Since the actions chosen by one user may influence the outcome for the other users in terms of probability of successful transmission, this can be framed as a stochastic game. For user i, if the channel gains of all the users in time slot t are $H_i(t)$, $G_i(t)$ and the action profile is (a_i, a_{-i}), we define its reward as,

$$\omega_i^{(t)}\left(a_i^{(t)}, H(t), G(t)\right) = \begin{cases} 1, & \text{if user } i \text{ receives an ACK,} \\ 0, & \text{otherwise.} \end{cases}$$

We are interested in the time average of the reward process

$$\nu_i\left(a_i, a_{-i}\right) = \limsup_{T\to\infty} \frac{1}{T}\sum_{t=1}^{T} \omega_i^{(t)}\left(a_i, H(t), G(t)\right). \tag{9}$$

We will restrict ourselves to Markov stationary policies, i.e., action of user i depends only on its current state $H_i(t), G_i(t)$. Then $\{\omega_i(a_i, H(t), G(t))\}$ are iid across time t. Hence by strong law of large numbers, the average reward $\nu_i(a_i, a_{-i}) = \mathrm{E}\left[\omega_i^{(t)}\left(a_i, H_i, G_i\right)\right]$ is same as the probability of successful transmission. In terms of a mixed strategy (ψ_i, ψ_{-i}), the average reward is

$$\nu_i\left(\psi_i, \psi_{-i}\right) = \sum_{a\in\mathcal{P}} \left[\prod_{j=1}^{K} \psi_{\pi(j)}\left(a_{\pi(j)}\right)\right] \nu_i\left(a_i, a_{-i}\right). \tag{10}$$

The objective of each user is to maximize its average reward (which is here the probability of successful transmission). Hence this stochastic game can be modelled as a one-shot game in which player i maximizes its utility (10). In the rest of the paper we develop algorithms to compute equilibrium points for this game.

III. Multiplicative Weight Algorithm for Learning CCE

In this section we use multiplicative weight algorithm ([10]) to compute an equilibrium point of the system. This is a distributed algorithm. The cost of each user can be defined as $c_i((a_i, a_{-i}) \triangleq -\nu_i(a_i, a_{-i})$. The algorithm provides coarse correlated equilibrium, defined below.

Definition: For an $\epsilon \geq 0$, if a distribution ψ on $\mathcal{P}$ satisfies

$$\mathsf{E}_{a\sim\psi}\left[C_i\left(a\right)\right] \leq \mathsf{E}_{a\sim\psi}\left[C_i\left(\hat{a}_i, a_{-i}\right)\right] + \epsilon, \tag{11}$$

for each i and actions $\hat{a}_i$, then it is called a $\epsilon-$ *coarse correlated equilibrium*. If we take $\epsilon = 0$, then it is simply called coarse correlated equilibrium (CCE).

A mixed-Nash equilibrium is a CCE. Hence for our finite game a CCE exists ([10]).

Definition:([10]) For user i, the external regret is defined as

$$\frac{1}{T}\sum_{t=1}^{T} \mathsf{E}_{a_{-i}\sim\psi_{-i}}\left[C_i^{(t)}\left(a_i^{(t)}, a_{-i}\right) - C_i^{(t)}\left(a_i, a_{-i}\right)\right] \tag{12}$$

for a given pure strategy sequence $a_i^{(1)}, \ldots, a_i^{(T)}$ with respect to an action a_i. In multiplicative weight algorithm, users update their strategies based on the cost received, such that the external regret converges to zero. This algorithm is presented in Algorithm 1. It converges to a CCE. ([10], [14]).

Algorithm 1 Multiplicative Weights Algorithm

do
  procedure Weight Update
    $w_i^{(t)}(a_i) \leftarrow 1, \ \forall\ a_i,\ i = 1, 2, \ldots, K$
    User i: Choose action $w.p.\ \Phi_i^{(t)} = \frac{\omega_i^{(t)}(a_i)}{\sum_{\hat{a}\in\mathcal{P}_i} w_i^{(t)}(\hat{a}_i)}$
Time t
    User i receives average utility for choosing a_i $\nu_i^{(t)} = \mathsf{E}_{a_{-i}\sim\Phi_{-i}}[C(a_i, a_{-1})]$
Update the weight
    $w_i^{(t+1)}(a_i) = w_i^{(t)}(a_i)(1-\epsilon)^{c_i^{(t)}(a_i)}$
Time $t+1$
    Calculate $\psi_t = \prod_{i=1}^{K} \Phi_i^{(t)}$
  end procedure
while $\frac{1}{T}\sum_{t=1}^{T} \mathsf{E}_{a_{-i}\sim\psi_{-i}}\left[C_i^{(t)}(a_i^{(t)}, a_{-i}) - C_i^{(t)}\left(a_i, a_{-i}\right)\right] > \epsilon$

Theorem 3.1: Let $\psi^{(t)} = \prod_{i=1}^{K} \Phi_i^{(t)}$ denote the outcome distribution at time t. There exist an integer $T > 0$ such that the regret of user i is less than ϵ after T iterations. Then, $\psi = \frac{1}{T}\sum_{t=1}^{T} \psi^{(t)}$ is an ϵ-coarse correlated equilibrium.

IV. Pareto Optimal Points

In a wireless environment it is realistic to assume that the ACK/NACK bits sent to a particular user can be successfully decoded by all the other users also (because these are sent at a low rate using robust codes). In that case all users can learn about the utility of each other at time t. We show in this section that this information can be used to get a socially optimal Pareto point which generally provides a better performance than a CCE.

Definition: An action profile $a \in \mathcal{P}$ is a *Pareto point* if there does not exist another profile $\tilde{a}$ such that $\nu_i(\tilde{a}) \geq \nu_i(a)$, $\forall\ i \in \mathcal{K}$ and $\nu_j(\tilde{a}) > \nu_i(a)$ for some $j \neq i$.

Define

$$\Omega(a) = \sum_{i=1}^{K} \gamma_i \nu_i(a), \tag{13}$$

for fixed $\gamma_i > 0,\ i = 1, \ldots, K$. Then a solution to the optimization problem

$$\max_{a} \quad \Omega(a), \quad \text{subject to } a \in \mathcal{P}. \tag{14}$$

is a Pareto point ([15]).

In Algorithm 2 below we provide a distributed algorithm in which the users update their strategies in a sequential fashion so as to improve $\Omega(a)$. This distributed algorithm is the variation of a heuristic stochastic local search algorithm. In this algorithm each user chooses a random action and uses it for a fixed number of time slots (say T). Then each user finds

the weighted sum of the utilities (since each user receives ACK/NACK of other users, it can calculate this quantity). After T slots one user experiments randomly and with some probability updates its action profile. This user uses this action for next T slots and while the other users use their previous action profiles. Comparing the weighted sum of utilities with the previous sum, it sets a new benchmark. The details of algorithm in the scenario of interference channel can be found in [11]. We present the detailed algorithm below as Algorithm 2.

Algorithm 2 Distributed Algorithm to obtain Pareto Points

User i: choose $a_i \in \mathcal{P}_i$ uniformly.
Use a_i for T time slots.
procedure WEIGHT UPDATE
    Update weight of each user i
    $\hat{\Omega}(a) \leftarrow \sum_{i=1}^{K} \gamma_i \left(\frac{1}{T} \sum_{t=1}^{T} \omega_i^{(t)}(a_i, H_i(t), G_i(t)) \right)$
    After T slots: $w.p\ \rho_i$ user i experiments
    procedure ACTION UPDATE
        $w.p\ \epsilon$ choose $a_i' \neq a_i$, $a_i' \in \mathcal{P}_i$
        $w.p.\ 1-\epsilon$
            choose $a_i' \neq a_i$ s.t. h_i with high α_i gets higher power level
        If α_i same for all h_i, then higher value of channel state gets higher power level.
    end procedure
    Call new action $\hat{a}_i$
    User i: use $\hat{a}_i$ for T time slots.
    $\hat{a}_j = a_j$ if user j is not experimenting.
    User i: find $\hat{\Omega}(\hat{a}_i, a_{-i})$

    if $\hat{\Omega}(\hat{a}_i, \hat{a}_{-i}) > \hat{\Omega}(a_i, \hat{a}_{-i})$ **then** $a_i \leftarrow \hat{a}_i$
        $P_{benchmark} = \hat{\Omega}(\hat{a}_i, \hat{a}_{-i})$
    else
        Randomly select another action
    end if
end procedure

V. NASH BARGAINING SOLUTION

The Pareto points obtained in Section IV are socially optimal, but may not be fair to all users: some users may get much more rates than others. To obtain fair Pareto points we use the concept of Nash Bargaining Solution (NBS) [16].

In NBS we need to specify a *disagreement* strategy and outcome that specifies the utility of each user that it receives by playing the disagreement strategy whenever there is no improvement over this utility in playing the bargaining outcome. We define the set of all possible utilities as

$$\mathcal{V} = \{(\nu_1(a), \ldots, \nu_K(a)) : a \in \mathcal{P}\}. \tag{15}$$

We also define the disagreement utility vector as $\delta = (\delta_1, \ldots, \delta_K)$ where δ_i is the utility obtained by player i if all players play the disagreement action Δ. The bargaining problem is denoted by $(\mathcal{V}, \delta)$.

The aim of the Bargaining problem is to find a bargaining solution which is Pareto optimal and satisfies the axioms of symmetry, invariance and independence of irrelevant alternatives ([16]).

Theorem 5.1 ([16]): There exists a unique bargaining solution (provided the feasible region is non-empty) obtained by the solution of the optimization problem:

$$\begin{aligned} &\max \ \prod_{i=1}^{K} (\nu_i - \delta_i) \\ &\text{subject to } \nu_i \geq \delta_i, i = 1, \ldots, K, \\ &(\nu_1, \ldots, K) \in \mathcal{V}. \end{aligned} \tag{16}$$

□

From [17], if the set of utilities $\mathcal{V}$ is convex then a Nash bargaining solution is also *proportionally fair*. In our problem $\mathcal{V}$ is convex and hence the solution is proportionally fair also.

VI. FADING MAC-WT WITH INDIVIDUAL MAIN CHANNEL CSI ONLY

We consider now the case where the users as well as the receiver do not know Eve's channel gain, but only its distribution. Also the transmitters *do not know even the distribution* of Eve's channel gains. In this scenario, the natural metric for the receiver to decide whether to send an ACK or a NACK will be outage based. First we define the secrecy outage, when $h_1, \ldots, h_K$ are given, as

$$\begin{aligned} &P_O^S(\pi(i)) \triangleq \\ &Pr\left\{ r_\pi(i) > \log\left(1 + \frac{h_{\pi(i)} P_{\pi(i)}(H_{\pi(i)})}{1 + \sum_{j=i+1}^{K} h_{\pi(j)} P_{\pi(j)}(H_{\pi(i)})}\right) \right. \\ &\left. - \log\left(1 + \frac{G_{\pi(i)} P_{\pi(i)}(H_{\pi(i)})}{1 + \sum_{j\neq i}^{K} G_{\pi(j)} P_{\pi(j)}(H_{\pi(j)})}\right) \right\}. \end{aligned} \tag{17}$$

The receiver sends an ACK if $P_o^S < \epsilon$, else the receiver sends a NACK. Hence we define utility of user i as

$$\omega_i\left(a_i^{(t)}, h_i(t)\right) = \mathbb{1}_{\{P_O^S(i) < \epsilon\}} \tag{18}$$

where $\mathbb{1}_{\{C\}}$ is an indicator function. With these utility functions, we can use the algorithms provided in Sections III-V.

VII. TRANSMISSION AT MULTIPLE RATES

Till now we have considered the case where the users are transmitting at fixed rates. Now we consider the more realistic scenerio where the users can transmit at different rates, depending on their channel gains. We assume that user i can choose any rate from the rate set $\mathcal{R}_i = \{r_i^{(1)}, \ldots, r_i^{(M_R)}\}$. We now define a new strategy set such that choosing the rate of transmission becomes a part of the action taken along with the power chosen by a user. Hence we define the modified strategy set as

$$\begin{aligned} &\mathcal{A}_i \triangleq \\ &\left\{(r_i, P_i^{(1)}, \ldots, P_i^{(M)}) : r_i \in \mathcal{R}_i, P_i^{(k)} \in \{p_i^{(1)}, \ldots, p_i^{(M)}\}, \right. \end{aligned}$$

$$\sum_{j=1}^{M} \alpha_i(j)\beta_i^{(j)} P_i^{(j)} \leq \overline{P}_i \Bigg\} \tag{19}$$

We can now use all the existing algorithms to compute a CCE, a PP and a NBS.

VIII. Avoiding Security Breach

In the previous sections we assumed that when the legitimate receiver cannot securely decode the message it sends a NACK. This is useful for the transmitters to learn the equilibrium point. But the messages transmitted during those slots may be decoded by Eve (with probability $> \epsilon$ in Section VI-A). Now we modify the system a little, so as to use the above coding scheme but mitigate this secrecy loss also.

We assume that each slot is comprised of two subslots. The fading process does not change during the whole slot. In the first part of the slot we transmit a dummy (random) message. If Bob sends an ACK to user i then the actual confidential message can be transmitted by user i in the second subslot at the same power. If Bob sends a NACK then user i should not use the second subslot. We can make the second subslot much larger than the first subslot so that the rate loss due to the dummy messages is minimal.

IX. Numerical Results

To compare the various schemes we first consider a 2-user fading MAC-WT with full CSI. We let $\mathcal{H} = \{0.1, 0.5, 0.9\}$ and $\mathcal{G} = \{0.05, 0.4, 0.8\}$ for both the users. We assume that the probability with which any state can occur is equal, i.e., $\alpha_i^j = \beta_i^j = 1/3$ for $i = 1, 2$, and $j = 1, 2, 3$. A user can choose any power from the power set $\{1, 5, \ldots, 100\}$. We first consider a fixed rate scenario. Each user knows its channel gain to Bob and Eve. We observe that the PP and the NBS obtain much higher sum rate than the CCE (Fig. 1). Also we observe that the NBS is fairer than the PP and the CCE (Fig. 2).

Next we consider the case where the users don't have CSI of Eve available but only the distribution is known. As in the previous example, here also we observe the same trend (Fig. 3, Fig. 4).

Next we consider the case when users have CSI of Eve available to them and can transmit at multiple rates choosing from $\{0.1,\ 0.2,\ 0.3,\ 0.4,\ 0.5,\ 0.6\}$. From Fig. 5 we note that PP and NBS give better secrecy sum-rates and from Fig. 6 we observe fairness of NBS.

We take one more example with $\mathcal{H} = \{0.1, .9\}$ and $\mathcal{G} = \{0.05, 0.8\}$. We compare the NBS and the PP with the case when CSI of the transmitters is known globally but only the distribution of Eve's channel gains are known at all transmitters. This case is studied in [8] for continuous channel states and a centralized solution which maximizes the sum rate is found. We also find the Bayesian Equilibrium (BE) for the case when each user knows distribution of all the channel gains to Eve, as done in [13] for F-MAC without security constraints. Here we observe that the NBS and the PP outperform BE at high SNR (Fig. 7). At low SNR the sum-rate for the NBS and the PP are quite close to that of BE. We also observe here that the CCE performs the worst.

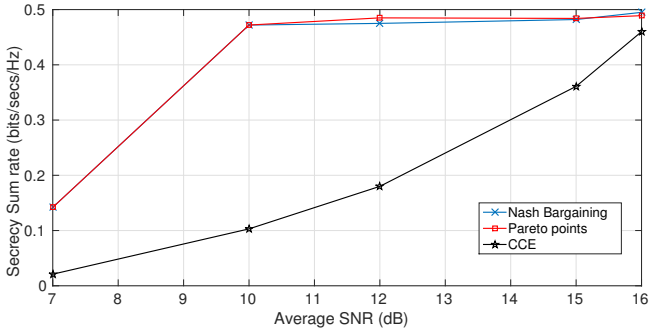

Fig. 1. Sum-rate with security constraints: comparison of CCE, PP and NBS at fixed transmission rate (with CSI of Eve).

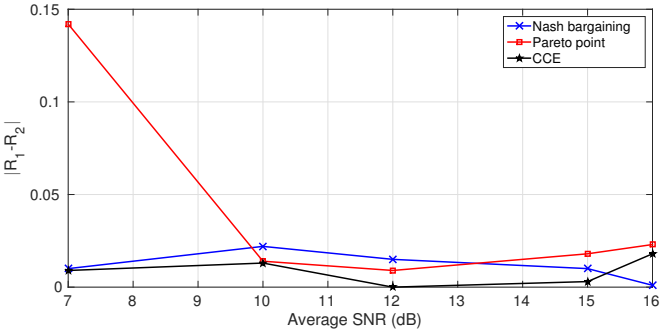

Fig. 2. Fairness of CCE, PP and NBS at fixed transmission rate (with CSI of Eve).

X. Conclusions

In this paper a K-user fading multiple access wiretap channel is studied. We first consider the case when each user knows only its channel gain to both the legitimate receiver and Eve. We propose the problem of power allocation as a

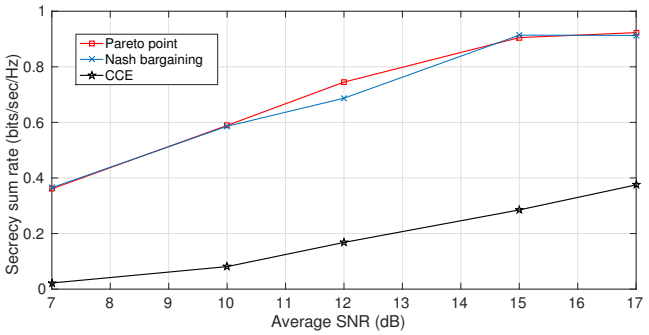

Fig. 3. Comparison of CCE, PP and NBS for F-MAC-WT, with no CSI of Eve (Fixed transmission rate).

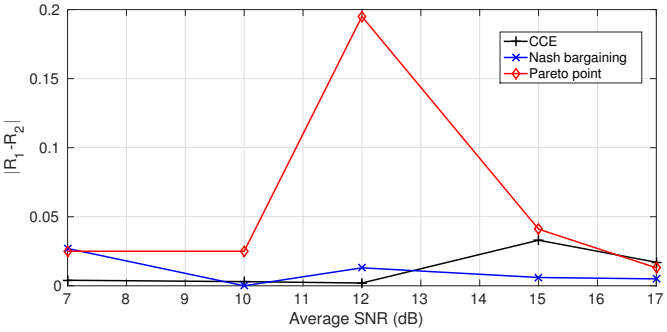

Fig. 4. Comparing fairness of CCE, PP and NBS for F-MAC-WT, with no CSI of Eve (Fixed transmission rate).

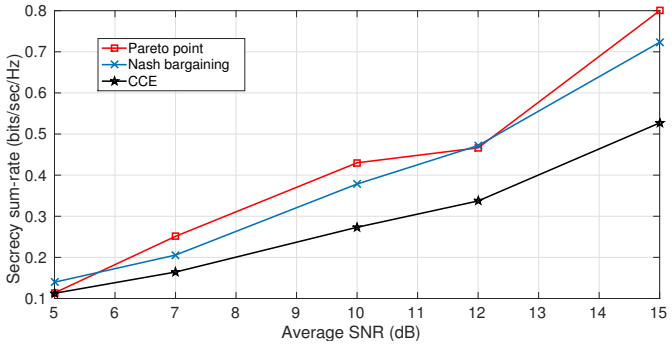

Fig. 5. FMAC-WT: Sum-rate comparison of CCE, PP and NBS for multiple rate case (with CSI of Eve).

stochastic game when the receiver sends an ACK or a NACK depending on whether it was able to decode the message or not. We used Multiplicative weight no-regret algorithm to obtain a Coarse Correlated Equilibrium (CCE). Then we consider the case when the users can decode ACK/NACK of each other. In that scenario we provide an algorithm to maximize the weighted sum-utility of all the users and obtain Pareto optimal point. PP is socially optimal but may be unfair to individual users. Next we consider the case where the users can cooperate with each other so as to disagree with the policy which will be unfair to individual user. We then obtain a Nash

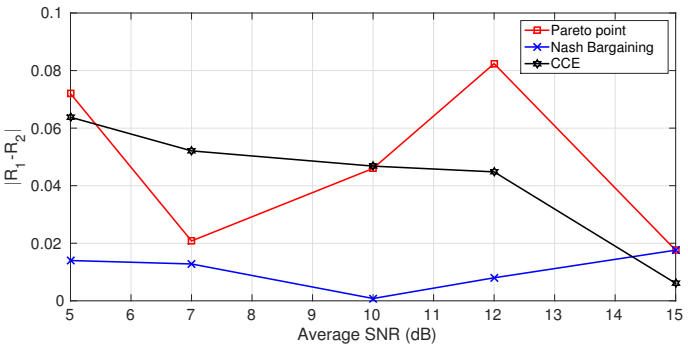

Fig. 6. F-MAC-WT: Fairness comparison of CCE, PP and NBS for multiple rate case (with CSI of Eve).

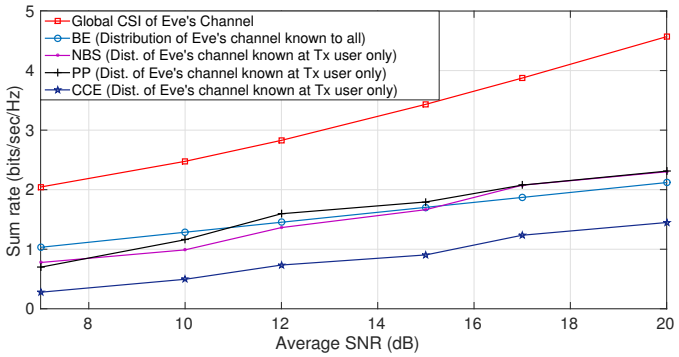

Fig. 7. F-MAC-WT: Comparing with existing schemes.

bargaining solution , which in addition to being Pareto optimal, is also fair to each user.

Next we consider the case where each user does not know the CSI of Eve but only its distribution. In that case we use secrecy outage as the criterion for the receiver to send an ACK or a NACK. Here also we use the previous algorithms to obtain a CCE, PP or a NBS. Finally we show that our algorithms can be extended to the case where a user can transmit at different rates. At the end we provide an example to compute different solutions and compare them under different CSI scenarios.

REFERENCES

[1] R. Liu, I. Maric, R. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Information Theory, 2006 IEEE International Symposium on*, July 2006, pp. 957–961.

[2] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 54, no. 3, pp. 976–1002, 2008.

[3] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Multiple access channels with generalized feedback and confidential messages," in *Information Theory Workshop, 2007. ITW'07. IEEE*. IEEE, 2007, pp. 608–613.

[4] E. Tekin and A. Yener, "The gaussian multiple access wire-tap channel," *Information Theory, IEEE Transactions on*, vol. 54, no. 12, pp. 5747–5755, 2008.

[5] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy," in *Information Theory Workshop (ITW), 2010 IEEE*. IEEE, 2010, pp. 1–5.

[6] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure dof of the single-antenna mac," in *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*. IEEE, 2010, pp. 2588–2592.

[7] H. Zivari-Fard, B. Akhbari, M. Ahmadian-Attari, and M. R. Aref, "Compound multiple access channel with confidential messages," in *Communications (ICC), 2014 IEEE International Conference on*. IEEE, 2014, pp. 1922–1927.

[8] S. M. Shah, V. Kumar, and V. Sharma, "Achievable secrecy sum-rate in a fading mac-wt with power control and without csi of eavesdropper," in *Signal Processing and Communications (SPCOM), 2012 International Conference on*. IEEE, 2012, pp. 1–5.

[9] N. Littlestone and M. K. Warmuth, "The weighted majority algorithm," *Information and computation*, vol. 108, no. 2, pp. 212–261, 1994.

[10] S. Arora, E. Hazan, and S. Kale, "The multiplicative weights update method: a meta-algorithm and applications." *Theory of Computing*, vol. 8, no. 1, pp. 121–164, 2012.

[11] K. A. Chaitanya, V. Sharma, and U. Mukherji, "Distributed learning of equilibria for a stochastic game on interference channels," in *Signal Processing Advances in Wireless Communications (SPAWC), 2015 IEEE 16th International Workshop on*. IEEE, 2015, pp. 650–654.

[12] L. Lai and H. El Gamal, "The water-filling game in fading multiple-access channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 5, pp. 2110–2122, 2008.
[13] G. He, M. Debbah, and E. Altman, "A bayesian game-theoretic approach for distributed resource allocation in fading multiple access channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, p. 8, 2010.
[14] N. Cesa-Bianchi and G. Lugosi, *Prediction, learning, and games*. Cambridge University Press, 2006.
[15] K. Miettinen, *Nonlinear multiobjective optimization*. Springer Science & Business Media, 2012, vol. 12.
[16] J. F. Nash Jr, "The bargaining problem," *Econometrica: Journal of the Econometric Society*, pp. 155–162, 1950.
[17] H. Boche and M. Schubert, "Nash bargaining and proportional fairness for wireless systems," *Networking, IEEE/ACM Transactions on*, vol. 17, no. 5, pp. 1453–1466, 2009.