Delay Constrained Secrecy Capacities in OFDMA Wireless Networks with Causal CSI

Arsenia **Chorti**[1,2] Katerina **Papadaki**[3], Panagiotis **Tsakalides**[1] and H. Vincent **Poor**[2]

[1]Institute of Computer Science, Foundation for Research and Technology-Hellas
[2]Department of Electrical Engineering, Princeton University
[3] Department of Management, London School of Economics
email: {achorti, poor} @princeton.edu, k.p.papadaki@lse.ac.uk, {achorti, ptsakalides} @ics.forth.gr

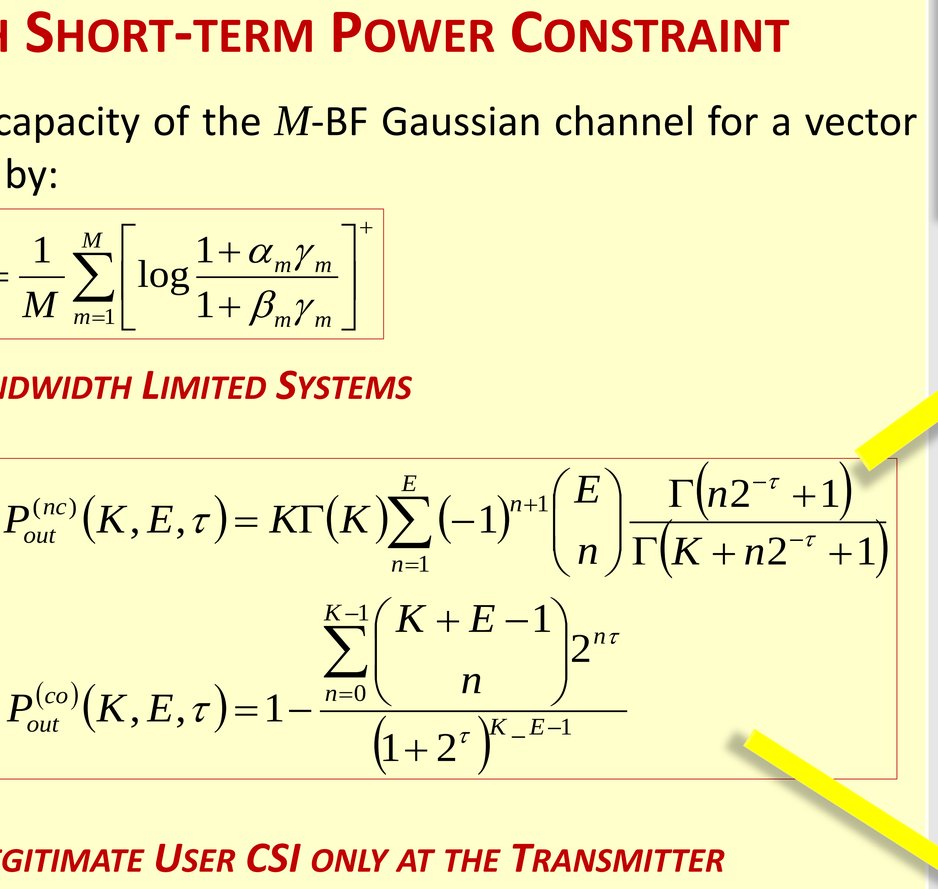
1. Introduction

OFDMA network with

- K legitimate users,
- E eavesdroppers,
- Max SNR channel allocation
- The k-th user is allocated $M^{(k)}$ channels

M block fading (BF) Gaussian channel with

- M blocks of N symbols
- N >> so that capacities are reached



2. Problem Formulation

We assume a Rayleigh channel with i.i.d. realizations $h_i^{(m)}$. Indices k^* and j^* denote the legitimate user and eavesdropper with the highest SNRs in the respective sets.

$$k_m^* = \arg\max \alpha_m, \alpha_m = \left|h_{k_m^*}^{(m)}\right|^2, m \in \{1,\ldots,M\}$$

$$j_m^* = \arg\max \beta_m, \beta_m = \left|h_{j_m^*}^{(m)}\right|^2, m \in \{1,\ldots,M\}$$

We transmit Gaussian codewords $\mathbf{x}_a$. The observation vectors at the respective receivers can be written as:

$$\mathbf{y}_a = \mathbf{H}_a\mathbf{x}_a + \mathbf{n}_a, \mathbf{H}_a = \mathrm{diag}\left(\mathbf{h}_{k_1^*}^{(1)}, \mathbf{h}_{k_2^*}^{(2)}, \ldots, \mathbf{h}_{k_M^*}^{(M)}\right),$$

$$\mathbf{y}_b = \mathbf{H}_b\mathbf{x}_a + \mathbf{n}_b, \mathbf{H}_b = \mathrm{diag}\left(\mathbf{h}_{j_1^*}^{(1)}, \mathbf{h}_{j_2^*}^{(2)}, \ldots, \mathbf{h}_{j_M^*}^{(M)}\right),$$

$$\mathbf{h}_i^{(m)} = h_i^{(m)}\mathbf{I}_N, i \in \left\{k_m^*, j_m^* : m = 1,\ldots,M\right\}$$

3. Power Control with Short-term Power Constraint

Definition: The instantaneous secrecy capacity of the M-BF Gaussian channel for a vector of input powers $\boldsymbol{\gamma}=(\gamma_1, \gamma_2, \ldots, \gamma_M)$ is given by:

$$C_s^{(M)} \doteq \frac{1}{M}\sum_{m=1}^{M}\left[\log\frac{1+\alpha_m\gamma_m}{1+\beta_m\gamma_m}\right]^+$$

- ***Probability of Secrecy Outage in Bandwidth Limited Systems***

In the high SNR region $\gamma_m \to \infty$ the probability of secrecy outage with respect to a threshold secrecy capacity τ is evaluated in the **absence of cooperation** and when **full diversity** is exploited. Numerical evaluations are given in Figs 1 and 2.

$$P_{out}^{(nc)}(K,E,\tau) = K\Gamma(K)\sum_{n=1}^{E}(-1)^{n+1}\binom{E}{n}\frac{\Gamma\left(n2^{-\tau}+1\right)}{\Gamma\left(K+n2^{-\tau}+1\right)}$$

$$P_{out}^{(co)}(K,E,\tau) = 1 - \frac{\sum_{n=0}^{K-1}\binom{K+E-1}{n}2^{n\tau}}{\left(1+2^{\tau}\right)^{K-E-1}}$$

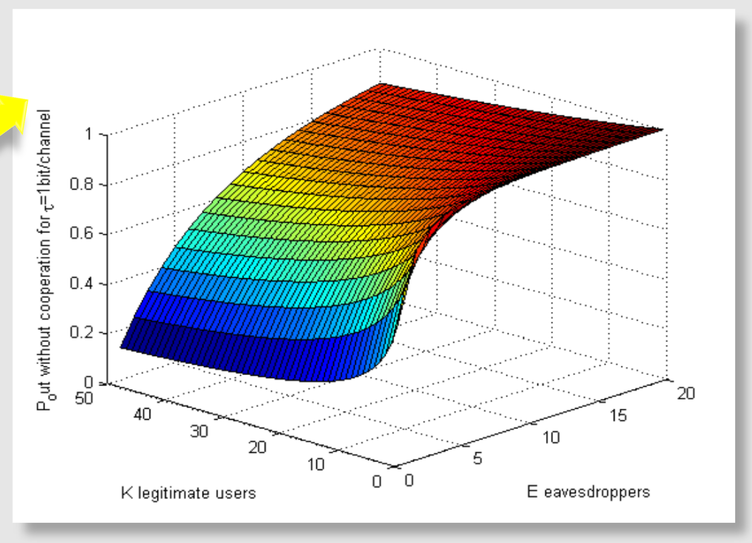


Fig 1: Probability of secrecy outage in the absence of cooperation

- ***One Sided Channel Inversion with Legitimate User CSI only at the Transmitter***

When M=1 and the legitimate user CSI is known at the transmitter only, we perform one-sided channel inversion under a frame based short-term power constraint P. Assuming the diversity is fully exploited, the secrecy capacity can be written as

$$\mathrm{E}\left[C_s^{(M)}\right] = \log\left(1+\frac{K-1}{K}P\right) - \int_0^{\infty}\int_0^{x}\log\left(1+\frac{y}{x}\frac{K-1}{K}P\right)\frac{KEx^{K-1}y^{E-1}e^{-x}e^{-y}}{(K-1)!(E-1)!}\mathrm{d}x\mathrm{d}y, \text{ with } \frac{1}{M}\sum_{m=1}^{M}\gamma_m \le P$$

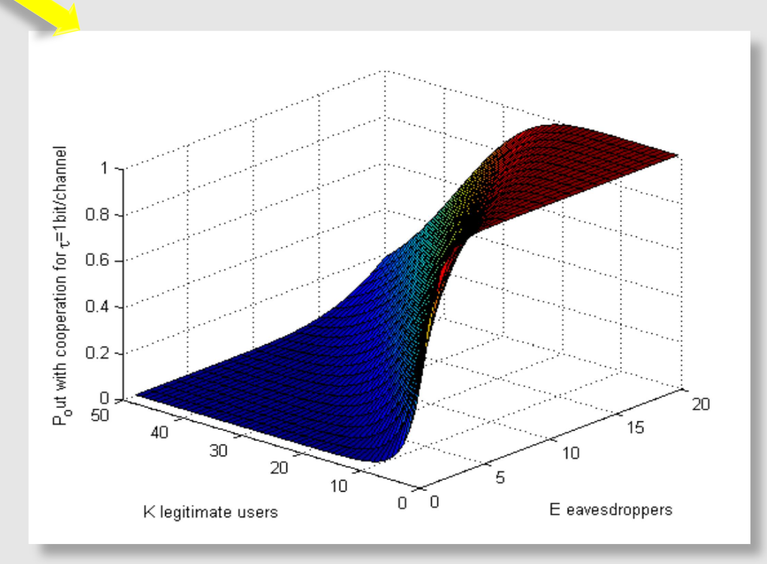


Fig 2:Probability of secrecy outage with full diversity

- ***Secure Water-filling with Full CSI at both the Transmitter and the Receiver***

We assume that the pairs of channel gains (α_m, β_m) are permuted so that the **differences** $\delta_m = \alpha_m - \beta_m$ **appear in non-decreasing order**. There exists a unique integer μ such that for $m > \mu$ the waterlevel is zero. Otherwise, the **shifted waterlevel** can be expressed as

$$\gamma_m^*\left(\frac{1}{\lambda}\right) + \frac{1}{\alpha_m} = \frac{1}{2}\left[\sqrt{\delta_m^2 + \frac{4}{\lambda}\delta_m} + \delta_m\right], m < \mu$$

4. Power Control with Block CSI and Long-term Power Constraint

We assume an **overall long-term** power constraint over T transmission frames in the form $T^{-1}\sum_{t=1}^{T}\gamma^{(t)} \le P$. We gain causal access to the channel gains at the best legitimate user during frame t, $\alpha^{(t)}$ and at the best eavesdropper during frame t, $\beta^{(t)}$. Our objective, given that we have remaining power p_t is to identify the power allocation that maximizes the instantaneous secrecy capacity and the secrecy capacity of future transmissions. We formulate the following **dynamic program**:

$$V_t(p_t) = \max_{0\le\gamma^{(t)}\le p_t}\mathrm{E}\left[R_s\left(\gamma^{(t)},\alpha^{(t)},\beta^{(t)}\right) + V_{t+1}\left(p_t-\gamma^{(t)}\right)\right],$$

$$\text{where } R_s\left(\gamma^{(t)},\alpha^{(t)},\beta^{(t)}\right) = \left[\log\frac{1+\alpha^{(t)}\gamma^{(t)}}{1+\beta^{(t)}\gamma^{(t)}}\right]^+, \text{ and } V_T(p_T) = 0 \text{ (resources exhausted)}$$