Optimal Power Allocation in Block Fading Gaussian Channels with Causal CSI and Secrecy Constraints

Arsenia Chorti, Katerina Papadaki, Harold Vincent Poor

Optimal Power Allocation in Block Fading Gaussian Channels with Causal CSI and Secrecy Constraints

Arsenia Chorti[†], Katerina Papadaki[‡], H. Vincent Poor[*]

[†]School of Computer Science and Electronic Engineering, Wivenhoe Park, Colchester, CO4 3SQ, UK
[‡]Department of Management, London School of Economics and Political Science, Houghton Street, London WC2A 2AE
[*]Department of Electrical Engineering, EQUAD, 19 Olden Street, Princeton University, Princeton, New Jersey 08544, USA
achorti@essex.ac.uk, k.p.papadaki@lse.ac.uk, {achorti, poor}@princeton.edu

***Abstract*—The optimal power allocation that maximizes the secrecy capacity (SC) of block fading Gaussian (BF-Gaussian) networks with causal channel state information (CSI), M-block delay tolerance and a frame based power constraint is examined. In particular, the SC maximization is formulated as a dynamic program. First, the SC maximization without any information on the CSI is studied; in this case the SC is maximized by equidistribution of the power budget, denoted as the "blind policy". Next, extending earlier results on the capacity maximization of BF-Gaussian channels without secrecy constraints, transmission policies for the low SNR and the high SNR regimes are proposed. When the available power resources are very low the optimal strategy is a "threshold policy". On the other hand when the available power budget is very large a "constant power policy" maximizes the frame secrecy capacity. Subsequently, a novel universal transmission policy is introduced, denoted in the following as the "blind horizon approximation" (BHA), by imposing a blind policy in the horizon of unknown events. Through numerical results, the novel BHA policy is shown to outperform both the threshold and constant power policies as long as the mean channel gain of the legitimate user is distinctively greater than the mean channel gain of the eavesdropper. Furthermore, the secrecy rates achieved by the BHA compare well with the secrecy rates of the secure waterfilling policy in the case of acausal CSI feedback to the transmitter.**

***Index Terms*—delay constrained secrecy capacity, causal CSI**

I. Introduction

Physical layer security (PLS) investigates the potential of taking advantage of the impairments in real communication media, such as fading or noise in wireless channels, in order to achieve confidentiality in data exchange. PLS was pioneered by Wyner, who introduced the wiretap channel and established the possibility of creating perfectly secure communication links without relying on private (secret) keys [1]. Recently, there have been considerable efforts devoted to generalizing this result to the wireless fading channel and to multi-user scenarios [2], [3].

In the present study we investigate optimal power allocation policies in block fading Gaussian (BF-Gaussian) wireless networks with secrecy and delay constraints. In our model, a transmitter wishes to broadcast secret messages to a legitimate user by employing physical layer security approaches, subject to a strict M-block delay constraint; accordingly, at the source a stochastic encoder maps the confidential messages to codewords of length $n = MN$ transmitted over M independent blocks, i.e., we assume that an interleaver of at most depth M is employed. We assume that the fading realizations are independent and identically distributed (i.i.d), that they remain constant over each block of N channel uses and that they change independently from one block to the next.

In the investigated setting, in order for random coding arguments to hold it is required that $n \to \infty$. For finite n, the BF-Gaussian channels are typically not information-stable and the generalized capacity expressions in [4] need to be employed. In this work, similarly to the work in [5], we bypass such issues by assuming that $N \to \infty$. The case of $M \to \infty$ that corresponds to the ergodic channel has been investigated in [2] and [6].

The presentation of our results is organized as follows. First, in Section II we restate the secure waterfilling solution to the optimal power allocation problem in M-block BF-Gaussian networks with acausal channel state information (CSI). This framework is pertinent to applications with parallel channels (e.g. in the frequency domain) under short-term power constraints (e.g. OFDM networks with frame based power constraints). Assuming that the M-block CSI is available at the transmitting and receiving nodes at the beginning of the transmission frame, the secure waterfilling policy that maximizes the network secrecy capacity [7] is discussed.

Next, in Sections IV and V we investigate BF-Gaussian channels with long term power constraints. We begin with a "blind scenario" in which the optimal power allocation is to be decided without any CSI information; the statistics of the channel gains are the only variables in the power allocation decision process. In absence of any CSI information we show that the optimal policy is to equally distribute the power budget in the M transmission blocks.

Then, we examine networks with causal access to the legitimate user's and the eavesdropper's CSI over a horizon of M transmission blocks; the pairs of the legitimate user's and eavesdropper's channel gains are sequentially revealed to the network nodes. We distinguish three subcases accounting for: (i) the low SNR regime, (ii) the high SNR regime, and, (iii) a novel universal approximation incorporating the blind scenario in the horizon of future events, denoted in the following as the "blind horizon approximation" (BHA).

This research was supported in part by the Marie Curie Outgoing Fellowship Program under Award FP7-PEOPLE-IOF-2010-274723, and in part by the U.S. National Science Foundation under Grant CMMI-1435778.

In the low SNR regime a threshold transmission policy is shown to be approximately optimal, in line with earlier results in networks without secrecy constraints [8]. On the contrary, in the high SNR regime the optimal strategy is to transmit with constant power in those blocks in which a non zero secrecy capacity can be achieved, in agreements with the results presented in [9] for the case without secrecy. Finally, using the BHA we derive a tractable expression for the transmission policy that depends quadratically on the remaining power and linearly on the gap between the legitimate and eavesdropping receivers' CSI. The derived policy is shown to outperform both the threshold and the constant power policy as long as the expectation of the gap between the legitimate and eavesdropping receivers' CSI is non-negligible.

II. System Model

We assume a BF-Gaussian channel with i.i.d. realizations. During the m-th transmission block the legitimate user's channel gain is denoted by α_m and the eavesdropper's channel gain by β_m. The proofs of the coding theorems will be included in the journal version of this paper.

Definition: The secrecy capacity density during one transmission block of the BF-Gaussian channel for an input power γ and channel gains (α, β) can be expressed as

$$c_s(\gamma, \alpha, \beta) \doteq \left[\log \frac{1+\alpha\gamma}{1+\beta\gamma}\right]^+ \tag{1}$$

with $[\cdot]^+ = \max(\cdot, 0)$. The secrecy capacity of the M-block transmission frame for a vector of input powers $\gamma = [\gamma_0, \gamma_1, \ldots, \gamma_{M-1}]$ and pairs of channel gains $(\alpha, \beta) = [(\alpha_0, \beta_0), (\alpha_1, \beta_1), \ldots, (\alpha_{M-1}, \beta_{M-1})]$, can be expressed as:

$$C_s \doteq \frac{1}{M} \sum_{m=0}^{M-1} c_s(\gamma_m, \alpha_m, \beta_m). \tag{2}$$

III. Power Control with Short-term Power Constraint and Full M-Block CSI

The optimal power allocation policy assuming that at the beginning of the transmission frame the CSI of M parallel blocks is revealed to the transmitting and receiving nodes has been derived in [2] and [7] and is repeated below for convenience. This is the baseline secure waterfilling policy and its performance cannot be exceeded in the causal scenario.

Without loss of generality we assume that the pairs of channel gains (α_m, β_m), $m = 0, \ldots, M-1$ are already permuted so that the differences

$$\delta_m = \alpha_m - \beta_m \tag{3}$$

appear in non-increasing order. The optimal power allocation problem can be stated as:

$$\max_{\gamma} C_s \tag{4}$$

$$\text{s.t.} \sum_{m=0}^{M-1} \gamma_m \leq MP \text{ and } \gamma_m \geq 0, m = 0, \ldots, M-1. \tag{5}$$

We further define the inverse channel gaps d_m as:

$$d_m = \frac{1}{\beta_m} - \frac{1}{\alpha_m}. \tag{6}$$

The power allocation $\gamma^* = (\gamma_0^*, \gamma_1^*, \ldots, \gamma_{M-1}^*)$ that maximizes the secrecy capacity satisfies the M-block power constraint with equality, i.e,

$$\sum_{m=0}^{M-1} \gamma_m^* = MP, \tag{7}$$

and is given by the secure waterfilling algorithm

$$\gamma_m^*\left(\frac{1}{\lambda}\right) = \begin{cases} \frac{1}{2}\left[\sqrt{d_m^2 + \frac{4}{\lambda} d_m} - \left(\frac{2}{\alpha_m} + d_m\right)\right], & m \in \mathbb{Q} \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

where $\mathbb{Q} = \{i : \lambda^{-1} \geq {\delta_i}^{-1}\}$.

The functions $\gamma_m^*(\lambda^{-1})$ are monotone increasing and continuous in λ^{-1}. As a result, there exists a unique integer μ in $\{0, \ldots, M-1\}$ such that $\lambda^{-1} \geq {\delta_m}^{-1}$ for $m \leq \mu$ and $\lambda^{-1} < {\delta_m}^{-1}$ for $m > \mu$. The waterlevel λ^{-1} can be derived by sequentially pouring water to the functions $\gamma_m^*(\lambda^{-1})$ until the power constraint is met with equality, i.e., $\sum_{m=0}^{\mu} \gamma_m^*(\lambda^{-1}) = MP$.

IV. Power Control with Long-term Power Constraint without CSI

We assume an overall long-term power constraint over M sequential transmission blocks in the form of (5). Accordingly, the channel gains of the legitimate user and the eavesdropper are assumed stationary over time with known expected values μ_α and μ_β respectively and realizations α_m and β_m during the m-th block. Our objective at block m, given that we have remaining power p_m, is the identification of the power allocation γ_m^* that maximizes the instantaneous secrecy capacity and the secrecy capacity for the future transmission blocks from block $m+1$ to M.

A. Blind Scenario

We first consider the case in which during the m-th block we take a decision on the value of γ_m without having information on the current channel gains (α_m, β_m), except for their stationarity over time and the remaining power p_m. In this formulation, our objective is to maximize the *expected* secrecy capacity over the entire horizon. In essence, this formulation corresponds to the case without delay and with perfect CSI at the receiver and no CSI at the transmitter ([5] Section II.A).

Let $\gamma = (\gamma_0, \ldots, \gamma_{M-1})$. The stochastic optimization objective function can be written as follows:

$$\max_{\gamma} \mathbb{E}\left\{\sum_{m=0}^{M-1} c_s(\gamma_m, \alpha_m, \beta_m)\right\} = \max_{\gamma} \mathbb{E}\left\{\sum_{m=0}^{M-1} c_s(\gamma_m, \alpha, \beta)\right\}, \tag{9}$$

where the expectation taken over the random variables α_m and β_m is re-written with rapport to the generic random variables α and β.

The above problem can be written as a stochastic dynamic program as follows: We let $V_m(p_m)$ (called the value function)

be the aggregate secrecy capacity density gained from block m to the end of the horizon if the optimal power allocation policy is used. Then the dynamic programming equations can be written as:

$$\begin{aligned} V_m(p_m) &= \max_{0\le\gamma_m\le p_m} \mathbb{E}\{c_s(\gamma_m,\alpha,\beta)+V_{m+1}(p_m-\gamma_m)\} \\ & \quad m=0,\dots,M \\ V_M(p_M) &= 0 \text{ (resources exhausted).} \end{aligned} \tag{10}$$

We perform backward dynamic programming on the optimality equations (10). We define the function:

$$f(\gamma) \equiv \mathbb{E}\left\{\left[\log\frac{1+\alpha\gamma}{1+\beta\gamma}\right]^+\right\}. \tag{11}$$

We start the dynamic programming recursion at block $m=M$, where the optimality equations are:

$$V_M(p_M) = \max_{0\le\gamma_M\le p_M} f(\gamma_M), \tag{12}$$

Since f is nondecreasing, the maximization in (12) is achieved at $\gamma_M^* = p_M$. Thus, we have: $\gamma_M^* = p_M$ and $V_M(p_M) = f(p_M)$. Thus, at block $m=M-1$ the optimality equations are:

$$V_{M-1}(p_{M-1}) = \max_{0\le\gamma_{M-1}\le p_{M-1}} f(\gamma_{M-1}) + f(p_{M-1}-\gamma_{M-1}). \tag{13}$$

Let $h(\gamma) = f(\gamma)+f(p-\gamma)$. Note that $h'(\gamma) = f'(\gamma) - f'(p-\gamma)$, and since $f'(\gamma)$ is nonincreasing and $f'(p-\gamma)$ is nondecreasing in γ, we have that h' is nonincreasing. This means that it can have at most one extreme point in the interval $[0,p]$, and the extreme point must be a maximum. At $\gamma=\frac{p}{2}$ we have: $h'\left(\frac{p}{2}\right) = f'(\frac{p}{2}) - f'(\frac{p}{2}) = 0$. Therefore in (13) the maximum is achieved at $\gamma_{M-1}^* = \frac{p_{M-1}}{2}$ and $V_{M-1}(p_{M-1}) = 2f(\frac{p_{M-1}}{2})$.

Continuing the recursion we get

$$V_{M-n}(p_{M-n}) = (n+1)f\left(\frac{p_{M-n}}{n+1}\right) \tag{14}$$

and the optimal decision is $\gamma_{M-n}^* = \frac{p_{M-n}}{n+1}$. This implies that if we have no information about the channel the optimal thing to do is to divide the power into as many equal parts as there are periods remaining, i.e., for $m=0,\dots,M-1$

$$\gamma_m^* = P. \tag{15}$$

The above results are intuitive; as expected, the blind maximization of a function of the outcomes of M independent trials can be achieved by equidistribution of the available resources.

V. Power Control with Long-term Power Constraint and Causal CSI

In the current section we investigate the case in which during the m-th transmission block we causally obtain information regarding the channel state, i.e., the pair (α_m,β_m) is causally revealed to the transmitter before the decision on γ_m is made. In this setting, during the m-th transmission block, we have to solve the following optimization problem:

$$\begin{aligned} V_m(p_m) &= \max_{\gamma_m\in\mathbb{A}} c_s(\alpha_m,\beta_m,\gamma_m) + \mathbb{E}\Big\{V_{m+1}(p_m-\gamma_m)\Big\} \\ \mathbb{A}_m &= \left\{\gamma_m : 0\le\gamma_m\le p_m \mathbb{1}_{\{\delta_m>0\}}\right\}. \end{aligned} \tag{16}$$

We distinguish two cases, according to the available power budget P; the low SNR and the high SNR regimes.

A. Low SNR Regime

In the low SNR regime, the available power is assumed small, i.e., $P\ll 1$. As a result a valid linear approximation of the logarithmic function would be $\log(1+z)\simeq z$, leading to an approximate expression for the secrecy capacity density given by:

$$c_s(\gamma,\alpha,\beta) \simeq [\alpha-\beta]^+\gamma = [\delta]^+\gamma, \tag{17}$$

with δ defined in (3). The value function V_m at $m=M$ could then be written as

$$V_M(p_M) = \max_{\gamma_M\in\mathbb{A}_M} [\delta_M]^+\gamma_M. \tag{18}$$

The secrecy capacity is thus approximated as a linear function of the power, so that at $m=M$ the optimal power allocation is straightforwardly given by

$$\gamma_M^* = \begin{cases} p_M, & \text{if } \delta_M>0, \\ 0, & \text{otherwise,} \end{cases} \tag{19}$$

which gives the following value function at $m=M$:

$$V_M(p_M) = [\delta_M]^+ p_M. \tag{20}$$

At $m=M-1$ the value function takes the form

$$\begin{aligned} V_{M-1}(p_{M-1}) &= \max_{\gamma_{M-1}\in\mathbb{A}_{M-1}} [\delta_{M-1}]^+\gamma_{M-1} \\ &+ \mathbb{E}\{[\delta]^+\}(p_{M-1}-\gamma_{M-1}). \end{aligned} \tag{21}$$

Thus, at $m=M-1$, the optimal power allocation is given by

$$\gamma_{M-1}^* = \begin{cases} p_{M-1}, & \text{if } [\delta_{M-1}]^+ > \mathbb{E}\{[\delta]^+\} \\ 0, & \text{if } [\delta_{M-1}]^+ \le \mathbb{E}\{[\delta]^+\} \end{cases} \tag{22}$$

Motivated by this result, the following near optimal power policy during the m-th block is proposed:

$$\gamma_m^* = \begin{cases} p_m, & \text{if } [\delta_m]^+ > \mathbb{E}\{[\delta]^+\} \\ 0, & \text{if } [\delta_m]^+ \le \mathbb{E}\{[\delta]^+\} \end{cases} \tag{23}$$

with $p_0 = MP$ and $m=0,\dots,M-1$. In the proposed threshold power policy, whenever a "good enough" gap in the channel gains δ_m of the legitimate and the eavesdropping receivers occurs then we transmit at full power.

Intuitively, in the low SNR regime there will not be many opportunities for achieving high values of the secrecy capacity density, so whenever such an opportunity occurs it should be seized in order to maximize the secrecy capacity over the whole horizon. The threshold is fixed to the expected value of the gap between the channel gains of the legitimate user and the eavesdropper, lower bounded by zero. Even when the legitimate user's channel is on average worse than the eavesdropper's, it is still possible to transmit at some non-zero rate even in the low SNR regime, given a long enough horizon, i.e., for large M.

B. High SNR Regime

In the high SNR regime, i.e., for $P \to \infty$, we can transmit at very high power during any of the transmission blocks. A good approximation for the secrecy capacity density during the m-th block is derived as

$$\lim_{\gamma\to\infty} c_s(\gamma,\alpha,\beta) = \left[\log\frac{\alpha}{\beta}\right]^+. \quad (24)$$

The maximization of the secrecy capacity is as a result independent of the power allocation and any transmission policy could be used. Accounting for other important considerations, e.g. the minimization of the information leakage, it is proposed to only transmit during the blocks that satisfy the condition $\delta_m > 0$, i.e.,

$$\gamma_m^* = \begin{cases} \frac{p_m}{M-m}, & \text{if } \delta_m > 0 \\ 0, & \text{if } \delta_m \le 0 \end{cases} \quad (25)$$

with $p_0 = MP$ and $m = 0,\ldots,M-1$.

VI. Blind Horizon Approximation (BHA)

In this section a novel universal approximation is derived by incorporating the blind policy in the horizon of future events. Suppose that we have the current CSI at block m, α_m and β_m when we take the power allocation decision γ_m. The optimality equations for this model are as follows:

$$\begin{aligned} V_m(p_m) &= \max_{\gamma_m\in\mathbb{A}_m} c_s(\alpha_m,\beta_m,\gamma_m) \\ &+ \mathbb{E}\Big\{V_{m+1}(p_m-\gamma_m)\Big\} \quad (26) \\ \mathbb{A}_m &= \Big\{\gamma_m : 0\le\gamma_m\le p_m \mathbb{1}_{\{\delta_m>0\}}\Big\}. \quad (27) \end{aligned}$$

The proposed approximation for V_m is given as:

$$\hat{V}_m(p_m) = \max_{\gamma_m\in\mathbb{A}_m} g_m(\gamma_m), \quad (28)$$

where g_m is as follows:

$$g_m(\gamma) = c_s(\alpha_m,\beta_m,\gamma) + (M-m)c_s\left(\mu_\alpha,\mu_\beta,\frac{p_m-\gamma}{M-m}\right), \quad (29)$$

with μ_α and μ_β being the expected values of the channel gains of the legitimate user and the eavesdropper respectively. The idea behind the BHA is to approximate the expected value of the secrecy capacity density in future time slots by assuming that (i) the channel gains will converge to their expected values, and, (ii) as a result of this the power allocation will be the blind policy due to symmetry.

A. Case I: $\alpha_m > \beta_m$ and $\mu_\alpha > \mu_\beta$

When $\alpha_m > \beta_m$ and $\mu_\alpha > \mu_\beta$ the function g_m can be rewritten as:

$$\begin{aligned} g_m(\gamma) &= \log\left(\frac{1+\alpha_m\gamma}{1+\beta_m\gamma}\right) \\ &+ (M-m)\log\left(\frac{1+\mu_\alpha\frac{p_m-\gamma}{M-m}}{1+\mu_\beta\frac{p_m-\gamma}{M-m}}\right) \quad (30) \end{aligned}$$

Taking $g_m'(\gamma) = 0$ gives the following roots:

$$(x_1,x_2) = \left(\frac{E+\sqrt{G}}{2F}, \frac{E-\sqrt{G}}{2F}\right) \quad (31)$$

where E and F are given below, G is given in the Appendix and for simplicity of notation we let $L_m = \frac{1}{M-m}$:

$$\begin{aligned} E &= 2\mu_\alpha\mu_\beta L_m^2(\alpha_m-\beta_m)p_m + [L_m(\alpha_m-\beta_m) \\ &\times (\mu_\alpha+\mu_\beta) + (\alpha_m+\beta_m)(\mu_\alpha-\mu_\beta)], \quad (32) \\ F &= \mu_\alpha\mu_\beta L_m^2(\alpha_m-\beta_m) - \alpha_m\beta_m(\mu_\alpha-\mu_\beta), \quad (33) \end{aligned}$$

We can show that $G \ge 0$ (the proof is omitted due to space limitations). Furthermore, x_1 is always outside the interval $[0,p_m]$ so that we always retain only root x_2. As a result we have the BHA power allocation given below (the proof can be found in the Appendix):

$$\gamma_m^* = \begin{cases} \min(x_2,p_m), & \text{if } (\alpha_m-\beta_m)\ge(\mu_\alpha-\mu_\beta) \\ \max(0,x_2), & \text{if } (\alpha_m-\beta_m)<(\mu_\alpha-\mu_\beta) \end{cases} \quad (34)$$

B. Case II: $\alpha_m > \beta_m$ and $\mu_\alpha \le \mu_\beta$

When $\alpha_m > \beta_m$ and $\mu_\alpha \le \mu_\beta$ the function g_m can be rewritten as:

$$g_m(\gamma) = \log\left(\frac{1+\alpha_m\gamma}{1+\beta_m\gamma}\right) \quad (35)$$

and the BHA reduces to the threshold policy so that

$$\gamma_m^* = p_m. \quad (36)$$

C. Case III: $\alpha_m \le \beta_m$

When $\alpha_m \le \beta_m$ the function g_m can be rewritten as:

$$g_m(\gamma) = (M-m)\log\left(\frac{1+\mu_\alpha\frac{p_m-\gamma}{M-m}}{1+\mu_\beta\frac{p_m-\gamma}{M-m}}\right) \quad (37)$$

and the optimal BHA policy is to allocate no power, i.e.,

$$\gamma_m^* = 0. \quad (38)$$

VII. Numerical results

In this section, we present numerical evaluations of the per block secrecy rates following the proposed transmission policies in Rayleigh channels, i.e., the channel gains α_m and β_m are exponentially distributed with mean values μ_α and μ_β respectively. We set $M = 10, \mu_\beta = 1$ and the average SNR per block as $\mu_\alpha P$. In Figs. 1-4 we depict the secrecy rates per block achieved by the various transmission strategies normalized to the benchmark secure waterfilling rate achieved with acausal CSI for $\mu_\alpha = \{0.1, 1.01, 5, 10\}$, averaged over 1000 channel realizations. We note that the waterfilling rate is not achievable in the case of causal CSI except for the asymptotic scenario of an ergodic channel with $M \to \infty$.

The threshold policy outperforms the constant policy in the low SNR regime and vice versa in the high SNR regime. Furthermore, the constant policy always outperforms the blind policy as in the latter part of the power budget is spent on blocks with zero secrecy capacity density when $\alpha_m \le \beta_m$.

On the other hand, for $\mu_\alpha \le \mu_\beta$ the BHA policy coincides with the threshold policy. In this case the BHA policy is not

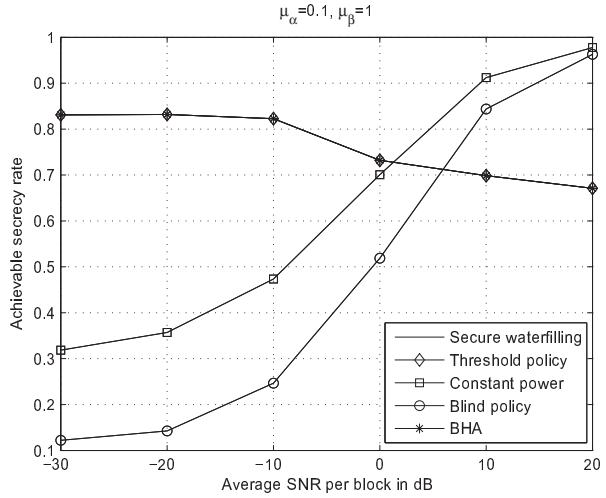

Fig. 1. Per block secrecy rates normalized to the secure waterfilling rate achieved by various policies for $\mu_\alpha = 0.1$, $\mu_\beta = 1$ and $M = 10$.

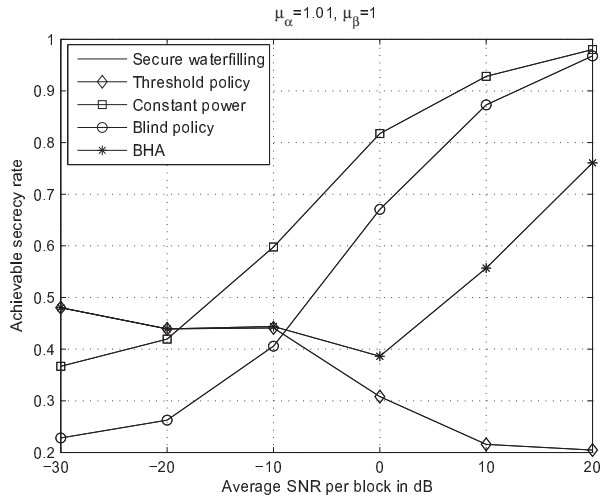

Fig. 2. Per block secrecy rates normalized to the secure waterfilling rate achieved by various policies for $\mu_\alpha = 1.01$, $\mu_\beta = 1$ and $M = 10$.

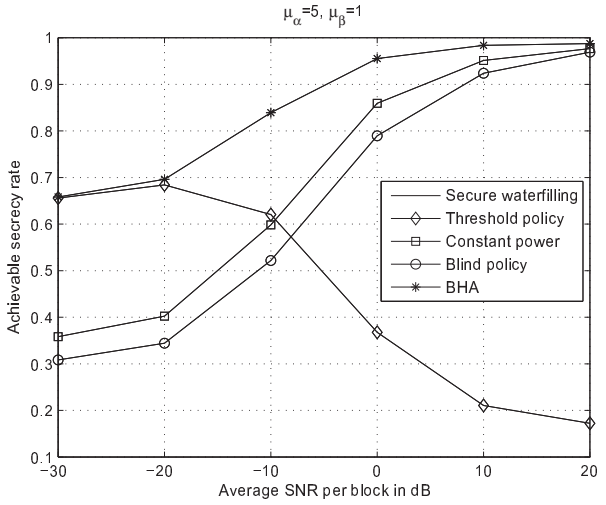

Fig. 3. Per block secrecy rates normalized to the secure waterfilling rate achieved by various policies for $\mu_\alpha = 5$, $\mu_\beta = 1$ and $M = 10$.

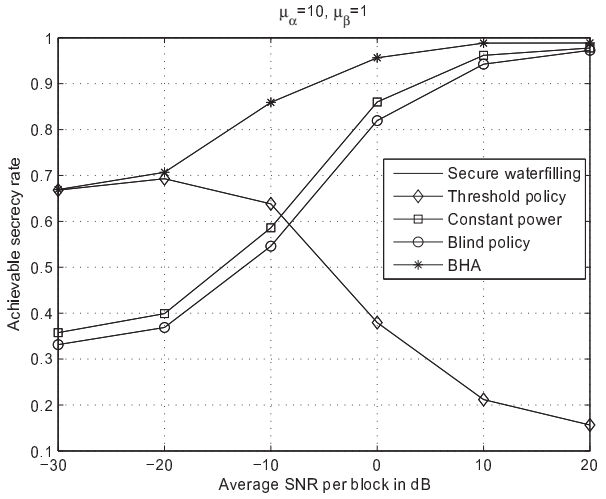

Fig. 4. Per block secrecy rates normalized to the secure waterfilling rate achieved by various policies for $\mu_\alpha = 10$, $\mu_\beta = 1$ and $M = 10$.

optimal in the whole SNR axis and is outperformed in the intermediate and high SNR regimes by the constant policy. The same is true for $\mu_\alpha \simeq \mu_\beta$. However, when μ_α is distinctly greater than μ_β the secrecy rate achieved with the BHA policy is greater than the rates achieved with the threshold and the constant policy over the entire SNR axis.

Finally, in Fig. 5 the average secrecy rates per block achieved by the causal BHA policy and the acausal waterfilling are depicted for $\mu_\beta = 1$ and $M = 10$. Interestingly, as long as μ_α is distinctly greater than μ_β, we loose almost no secrecy rate -in absolute terms- due to the causal nature of the CSI feedback over the entire SNR axis.

VIII. Conclusions

We have investigated the optimal power allocation in delay constrained M-block BF-Gaussian networks. By studying the blind case with no CSI availability during the decision process we have concluded that the optimal policy consists of equally distributing the power along the transmission blocks. Furthermore, the study of networks with causal access to the CSI has been performed accounting for three distinct cases; the low and the high SNR regimes and a novel universal approximation. In the low SNR regime we have proposed a near optimal threshold policy whereas in the high SNR regime a constant transmission policy has been shown to be near optimal. Finally, by incorporating the blind policy in the horizon of future events we have been able to derive a novel universal approximation that we have denoted as "the blind horizon approximation" (BHA). Through numerical evaluations it has been shown that the BHA compares favorably with the benchmark waterfilling policy in the acausal feedback case and consistently outperforms the threshold and constant power transmission policies as long as the mean channel gain of the legitimate user is distinctively greater than the mean channel gain of the eavesdropper.

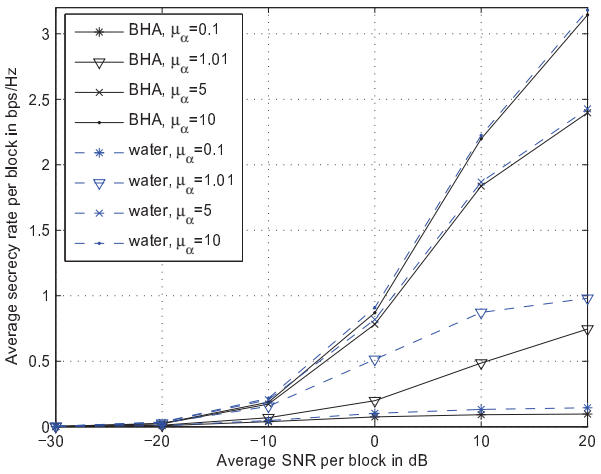

Fig. 5. Average secrecy rates per block achieved by the BHA policy and the waterfilling policy for $\mu_\beta = 1$ and $M = 10$.

IX. Appendix

The expression for G is given in (39) below. It can be shown that when $\alpha_m > \beta_m$ and $\mu_\alpha > \mu_\beta$, $G \geq 0$.

Next we prove that x_1 is always outside the interval $[0, p_m]$. We have two cases, according to the sign of F. For $F > 0$, it is straightforward to show that $x_1 \geq \frac{E}{2F} > p_m$, since the coefficient of p_m in the ratio $\frac{E}{2F}$ is greater than or equal to 1 and the constant term is strictly positive. Thus, if $F > 0$ then $x_1 > p_m$. On the other hand for $F < 0$, $x_1 < 0$, since $E + \sqrt{G}$ is strictly positive. Therefore, x_1 is always outside the interval $[0, p_m]$.

Regarding whether x_2 is in the interval $[0, p_m]$ we first calculate the derivative of g_m at points 0 and p_m, given in (40) and (41) below. If $(\alpha_m - \beta_m) \geq (\mu_\alpha - \mu_\beta)$, then $g'_m(0) \geq 0$. Since only one root of g'_m can exist in the interval $[0, p_m]$, namely x_2, if $g'_m(p_m) \geq 0$ then the root (maximum) must be outside of the interval $[0, p_m]$, $x_2 \geq p_m$, and the maximum is achieved at p_m. However, if $g'_m(p_m) < 0$ then the root must be in $[0, p_m]$ and the maximum is achieved at x_2. Thus the maximum in $[0, p_m]$ is achieved at $\min(x_2, p_m)$.

If on the other hand $(\alpha_m - \beta_m) < (\mu_\alpha - \mu_\beta)$, then $g'_m(p_m) \leq 0$. Since only one root of g'_m can exist in the interval $[0, p_m]$, namely x_2, if $g'_m(0) \leq 0$ then the root (the maximum) must be outside of the interval $[0, p_m]$, $x_2 \leq 0$ and the maximum is achieved at 0. However, if $g'_m(0) > 0$ then the root must be in $[0, p_m]$ and the maximum is achieved at x_2. Thus the maximum in $[0, p_m]$ is achieved at $\max(0, x_2)$. This gives the power allocation in (34).

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1385–1357, Oct. 1975.

[2] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Information Theory*, vol. 6, no. 54, pp. 2470–2492, Jun. 2008.

[3] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "On the resilience of wireless multiuser networks to passive and active eavesdroppers," *IEEE J. Selected Areas in Communications*, vol. 31, no. 9, p. 1850, Sep. 2013.

[4] S. Verdú and T. S. Han, "A general formula for channel capacity," *IEEE Trans. Information Theory*, vol. 40, no. 4, pp. 1147–1157, Jul. 1994.

[5] G. Caire, G. Taricco, and E. Biglieri, "Optimum power control over fading channels," *IEEE Trans. Information Theory*, vol. 45, no. 5, pp. 1468–1489, Jul. 1999.

[6] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Information Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[7] A. Chorti, K. Papadaki, P. Tsakalides, and H. V. Poor, "The secrecy capacity of block fading multiuser wireless networks," in *Proc of the IEEE International Conference on Advanced Technologies for Communications (ATC'13)*. Ho-Chi Minh City, Vietnam: IEEE, Oct. 2013, pp. 247 – 251.

[8] R. Negi and J. M. Cioffi, "Delay-constrained capacity with causal feedback," *IEEE Trans. Information Theory*, vol. 48, no. 9, pp. 2478–2494, Sep. 2002.

[9] X. Liu and A. J. Goldsmith, "Optimal power allocation over fading channels with stringent delay constraints," in *Proc. of the IEEE International Conference on Global Communications (GLOBECOM'02)*, Tapei, Taiwan, 17-21 Nov. 2001, pp. 1413–1418.

$$
\begin{aligned}
G &= (\alpha_m - \beta_m)[-4\alpha_m\mu_\beta^2\beta_m\mu_\alpha L_m^2 p_m^2 + 4\alpha_m\mu_\alpha^2\beta_m L_m^2 p_m^2\mu_\beta - \mu_\beta^2\beta_m + \alpha_m\mu_\beta^2 - \mu_\alpha^2\beta_m + \mu_\alpha^2\alpha_m \\
&- 4\alpha_m\mu_\beta^2\mu_\alpha L_m^2 p_m - 4\alpha_m\mu_\beta^2 b L_m p_m + 4\alpha_m\mu_\alpha^2\beta_m L_m p_m + 4\alpha_m\mu_\alpha^2 L_m^2 p_m\mu_\beta - 4\beta_m\mu_\beta^2\mu_\alpha L_m^2 p_m \\
&+ 4\beta_m\mu_\alpha^2 L_m^2 p_m\mu_\beta - \mu_\alpha^2 L_m^2\beta_m + \alpha_m\mu_\alpha^2 L_m^2 + \alpha_m L_m^2\mu_\beta^2 - \beta_m L_m^2\mu_\beta^2 - 2\alpha_m\mu_\alpha L_m^2\mu_\beta + 2\beta_m\mu_\alpha L_m^2\mu_\beta \\
&- 2\alpha_m\mu_\beta^2 L_m - 2\beta_m\mu_\beta^2 L_m - 4\mu_\beta\alpha_m\beta_m + 4\mu_\alpha^2 L_m^2\mu_\beta - 4\mu_\alpha L_m^2\mu_\beta^2 + 2\beta_m\mu_\alpha\mu_{\beta_m} + 2\alpha_m\mu_\alpha^2 L_m \\
&+ 2\beta_m\mu_\alpha^2 L_m + 4\mu_\alpha\alpha_m\beta_m - 2\alpha_m\mu_\alpha\mu_\beta]. \qquad (39)
\end{aligned}
$$

$$
g'_m(0) = \frac{[\mu_\alpha\mu_\beta L_m^2(\alpha_m - \beta_m)]p_m^2 + [L_m(\alpha_m - \beta_m)(\mu_\alpha + \mu_\beta)]p_m + [(\alpha_m - \beta_m) - (\mu_\alpha - \mu_\beta)]}{(1 + \mu_\alpha L_m p_m)(1 + \mu_\beta L_m p_m)} \qquad (40)
$$

$$
g'_m(p_m) = \frac{[-\alpha_m\beta_m(\mu_\alpha - \mu_\beta)]p_m^2 + [-(\mu_\alpha - \mu_\beta)(\alpha_m + \beta_m)]p_m + [(\alpha_m - \beta_m) - (\mu_\alpha - \mu_\beta)]}{(1 + \alpha_m p_m)(1 + \beta_m p_m)} \qquad (41)
$$