Arsenia Chorti, Katerina Papadaki, and Vincent Poor

Optimal power allocation in block fading channels with confidential message

Article (Accepted version) (Refereed)

Original citation:
Chorti, Arsenia, Papadaki, Katerina and Poor, H. Vincent (2015) Optimal power allocation in block fading channels with confidential messages. IEEE Transactions on Wireless Communications, PP (99). p. 1. ISSN 1536-1276

DOI: 10.1109/TWC.2015.2424964

Optimal Power Allocation in Block Fading Channels with Confidential Messages

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

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

***Abstract*—The optimal power allocation for block fading (BF) networks with confidential messages is investigated under an M-block delay and power constraint. First, we study networks without channel state information (CSI) feedback to the transmitter and demonstrate that the optimal power allocation is the equidistribution of the power budget, denoted as the "blind policy". In blind scenarios secrecy can be achieved though receiver diversity; the probability of secrecy outage (PSO) is shown to decay exponentially with the the diversity order of the legitimate user. Then, we investigate networks with CSI feedback. For comparison purposes, we restate the acausal secure waterfilling algorithm with full CSI before moving to the causal feedback scenario. In the latter, an approximate "threshold policy" for the low SNR and an approximate "high power policy" for the high SNR regimes are derived. Furthermore, a novel universal transmission policy is proposed across all SNRs, denoted as the "blind horizon approximation" (BHA). Through numerical results, the BHA policy is shown to outperform both the threshold and high power policies when the legitimate user has an SNR advantage with respect to the eavesdropper, while it also compares well with the secure waterfilling policy.**

***Index Terms*—Secrecy capacity, probability of secrecy outage, block fading, BF-AWGN channel, causal channel state information feedback, dynamic program**

I. Introduction

The increasing deployment of wireless networks introduces new challenges in the design of enhanced security next generation systems. A pressing need to develop alternative/complementary means to secure data exchange arises in many wireless settings with limited feedback and limited resources. Physical layer security (PLS) is an emerging technology from the area of information theory that can address open security issues in challenging wireless applications such as those envisaged for fifth generation (5G) networks. In PLS approaches [1], the issues of reliability and secrecy in the exchange of information are jointly addressed by employing novel double binning encoding schemes.

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 [2]. Wyner termed the rates at which information can be transmitted secretly from the source to its intended destination as achievable secrecy rates, and the maximal achievable secrecy rate as the secrecy capacity (SC). Following Wyner's contribution, the SC of the scalar Gaussian wiretap channel was analyzed in [3]. In [4], Wyner's approach was generalized to the transmission of confidential messages over broadcast channels. Renewed interest in the area over the last two decades led to the characterization of the SC of the quasi-static fading channel in [5], followed by the characterization of the delay unconstrained SC of the ergodic fading channel in [6]. In parallel, in [7], the capacity-equivocation region of the generic parallel broadcast channel with confidential messages (BCC) was derived and the results were applied to various classes of broadcast channels (including the ergodic fading channel). Furthermore the rapidly expanding literature on PLS topics, includes contributions for: multiple input multiple output (MIMO) systems [8], [9], interference and multiple access channels [10], [11], multi-user scenarios [12], and relay and cooperative networks [13], [14] while in [15] a novel triple binning scheme using standard QAM modulators to achieve strong secrecy in PNC applications has been developed, to cite but a few.

In this contribution we investigate the SC and the probability of secrecy outage (PSO) of block fading additive white Gaussian noise (BF-AWGN) channels (i) without feedback or (ii) with causal feedback of the channel state information (CSI) to the transmitter. The general class of BF-AWGN channels without confidential messages was investigated in [16], [17], [18] and [19]. Previous work on the secrecy rates of BF channels have looked at different aspects of the topic. For example, in [20] the secrecy degrees of freedom of multi-antenna block fading (BF) coefficients were investigated by exploiting the temporal correlation of the BF channels seen by different receivers. Furthermore, in [21] distributed systems with linear precoding were studied while in [22] point-to-point secure communication over flat fading channels under outage constraints were considered. In the same contribution capacity achieving schemes based on opportunistically exchanging private keys between the legitimate nodes were proposed. Furthermore, in [23] the SC of the ergodic BF wiretap channel with partial CSI at the transmitter and perfect CSI at the receivers was studied.

Our work differs from previous contributions as we explicitly focus on delay constrained BF-AWGN channels, as opposed to ergodic scenarios. In particular with respect to the ergodic scenario, [6] and [7] presume that all channel realizations occur during encoding, whereas in our investigation (i) we consider the more realistic setting in which only a finite number of channel realizations occur during encoding, and,

(ii) the channel realizations can be either sequential in time or parallel (instead of strictly parallel), i.e., we explicitly look into causal channels as well. In the investigated system model a source wishes to broadcast to an intended destination secret messages which are spread over M blocks of N symbols. Each block of N symbols is assumed to undergo the same channel state (fading); 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. The fading realizations are modeled to be independent and identically distributed (i.i.d) random variables, i.e., they remain constant over each block of N channel uses and change independently from one block to the next.

For $M = 1$, this study reduces to the quasi-static fading channel [5], while for $M \to \infty$ the delay unconstrained ergodic fading channel arises [6], [7]. For finite M, the BF-AWGN channel is typically not information-stable. By letting $N \to \infty$ though, we can give operational meaning to the concept of the delay limited SC which is closely related to the PSO; in agreement to intuition we remark that the delay limited SC is the rate that minimizes the PSO. This result is very useful as it allows to convert a non-convex optimization problem - that of minimizing the PSO - to a convex optimization problem - that of maximizing the delay limited SC.

To the best of our knowledge, the present paper presents the first systematic study of the following aspects of BF-AWGN channels with secrecy and delay constraints:

- *Systems without CSI feedback*: Absence of CSI feedback is typical in broadcasting applications with multiple destinations or one-way networks consisting of a large number of resource limited devices, e.g., sensor networks, etc. In the "blind" scenario we formulate the problem of maximizing the expected value of the secrecy rate as a dynamic program (DP) and derive an analytic solution, which states that the optimal resource allocation is to equally distribute the overall power budget across all M-blocks. We refer to this as the "blind transmission policy" and provide novel closed form expressions for the PSO as a function of the diversity orders of the legitimate user and the eavesdropper in the generic multi-antenna or multi-user setting. An interesting outcome of this investigation is that for small secrecy rates the PSO decays exponentially with the diversity order of the legitimate user.

- *Systems with causal CSI feedback*: Causal CSI feedback is typical in time division channels. Additionally, the full CSI may be available to the source in networks consisting of benign nodes with different access rights to the transmitted information [24], i.e., when the eavesdropper is a legitimate node in the network not authorized to receive certain content. Using the assumption that the full CSI is revealed to the transmitter causally before the decision on the power allocation is made, we formulate the problem as a DP. However, unlike the "blind" case, we cannot derive analytical solutions for the DP. Thus, we use the DP formulation to derive three distinct sub-optimal resource allocation policies that correspond to (i) a low SNR regime, (ii) a high SNR regime, and (iii) a universal policy that incorporates the blind policy in the horizon of future events, denoted as the blind horizon approximation (BHA). The proposed sub-optimal policies are given in closed form and require only a few operations (e.g. comparisons and multiplications). As a result, the proposed policies are very well suited for resource limited, real-time applications such as device-to-device communications envisaged for 5G networks.

- *Feasibility of PLS in BF-AWGN channels*: Through the present study, the effect of diversity in time or frequency when $M > 1$ in the acausal and causal feedback scenarios or the multi-user or multi-antenna diversity in the blind scenario are shown to have an important impact on the feasibility of secrecy. In blind scenarios, we demonstrate that cooperative wireless networks can be robust to passive attacks when the diversity order of potential adversaries can be upper bounded. On the other hand, when either acausal or causal feedback is available, diversity in the time/frequency can accommodate secrecy rates compatible with many actual wireless systems.

The paper is organized as follows: Section II introduces the system model and the delay limited SC and PSO in BF-AWGN channels. In Section III the formulation of the power allocation problem using DP is given. In Section IV, for comparison purposes, the full acausal CSI feedback scenario in which both the legitimate user's and the eavesdropper's CSIs are acausally available to the transmitter is revisited and the results of the authors' contribution in [25] are restated. In section V the case of causal CSI feedback is investigated and approximate policies for the low, high and universal SNR regimes are derived using the DP formulation. An extensive set of numerical evaluations is presented in section VII. Finally, the conclusions of this study are summarized in section VIII where also future research directions are discussed.

II. Delay Limited Secrecy Capacity and Probability of Secrecy Outage

We assume a memoryless BF-AWGN channel with i.i.d. realizations and three nodes of interest; a source node, a legitimate user and an eavesdropper. Each transmission block is assumed to be a general broadcast channel from the source node to the two receivers. The source node wants to transmit confidential information to the legitimate user in the presence of the eavesdropper at the maximal possible rate. At the transmitter front-end an I-Q modulator is employed and as a result two independent real transmission paths are available during each transmission slot due to the employment of two orthogonal signalling carriers (e.g. a sine and a cosine wave). As a result, the capacity expressions that hold for real channels are scaled by a factor of 2. Keeping this in mind, in the following we will assume that all random variables are real but drop the coefficient $\frac{1}{2}$ in the capacity expressions. Finally, all logarithms hereafter are assumed base 2.

Information exchange occurs in frames, each frame consisting of M transmission blocks of N symbols. In one frame, the vectors of channel gains at the intended and eavesdropping receivers are denoted by $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_M)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_M)$ respectively; during the m-th transmission block the legitimate user's channel fading coefficient is $\sqrt{\alpha_m}$, while the eavesdropper's channel fading coefficient is $\sqrt{\beta_m}$.

Finally, in the following the variance of all additive white Gaussian noise (AWGN) sources is normalized to unity for convenience, i.e., the effect of AWGN is incorporated into the channel gains.

Let $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{w}, \tilde{\boldsymbol{w}}$ be vectors in $\mathbb{R}^{MN}$ with $\boldsymbol{x} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_M)^T$, $\boldsymbol{y} = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_M)^T$, $\boldsymbol{z} = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_M)^T$, $\boldsymbol{w} = (\boldsymbol{w}_1, \ldots, \boldsymbol{w}_M)^T$, $\tilde{\boldsymbol{w}} = (\tilde{\boldsymbol{w}}_1, \ldots, \tilde{\boldsymbol{w}}_M)^T$ where $\boldsymbol{x}_m, \boldsymbol{y}_m, \boldsymbol{z}_m, \boldsymbol{w}_m, \tilde{\boldsymbol{w}}_m$ are vectors in $\mathbb{R}^N$ for $m = 1, \ldots, M$. During one frame, the outputs of optimal receivers at the intended destination, denoted by $\boldsymbol{y}$, and at the eavesdropper, denoted by $\boldsymbol{z}$, are expressed, respectively, as follows:

$$\boldsymbol{y} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{w}, \tag{1}$$

$$\boldsymbol{z} = \boldsymbol{B}\boldsymbol{x} + \tilde{\boldsymbol{w}}, \tag{2}$$

with $\boldsymbol{A} = \mathrm{diag}(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_M})$ an $M \times M$ diagonal matrix whose elements are the legitimate destination's fading amplitudes and $\boldsymbol{B} = \mathrm{diag}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_M})$ an $M \times M$ diagonal matrix whose elements are the eavesdropper's fading amplitudes. The construction of the codeword $\boldsymbol{x}$ is explained in detail in subsection II-A while the terms $\boldsymbol{w}$ and $\tilde{\boldsymbol{w}}$ are vectors whose components are zero-mean unit-variance circularly symmetric Gaussian random variables.

Due to the memoryless assumption in the modeling of the fading coefficients, the channel output transition probability distribution is factored over the M independent blocks and is given by

$$p(\boldsymbol{y}, \boldsymbol{z}|\boldsymbol{x}) = \prod_{m=1}^{M} p(\boldsymbol{y}_m, \boldsymbol{z}_m|\boldsymbol{x}_m). \tag{3}$$

As a result of (3) the M-block BF-AWGN channel is equivalent to the M-parallel broadcast channel with confidential messages (eq. (1) in [7]).

A. Delay Limited Secrecy Capacity

During each transmission frame, the transmitter wishes to convey to the intended destination a message $\boldsymbol{s} = (s(1), \ldots, s(q)) \in \mathcal{S}^q$, whose elements are uniformly drawn from a set of source symbols $\mathcal{S}$. To this end, the source employs a (stochastic) encoder described by the mapping $\varphi : \mathcal{S}^q \to (\mathcal{X}_1^N, \ldots, \mathcal{X}_M^N)$, with $\mathcal{X}_m$ the m-th encoder alphabet. At the intended destination, at the end of the transmission frame, the decoding function $\phi : (\mathcal{Y}_1^N, \ldots, \mathcal{Y}_M^N) \to \mathcal{S}^q$ is used to recover the source symbols from the observations. The error probability associated with the code (φ, ϕ) is defined as

$$P_e = \Pr\left(\phi(\boldsymbol{y}) \neq \boldsymbol{s}\right). \tag{4}$$

The level of ignorance of the eavesdropper with respect to the transmitted message is measured by its equivocation rate R_e,

$$R_e = \frac{1}{n} H(\boldsymbol{S}|\boldsymbol{Z}). \tag{5}$$

In the following, we focus on information theoretic weak secrecy, implying that the equivocation rate is at least equal to the rate of the message denoted by R_s. Perfectly secret transmission at rate R_s is achieved if for any arbitrarily small $\epsilon > 0$, there exists a sequence of codes $(2^{nR_s}, n)$ such that for $n \to \infty$, the following hold [2], [4]:

$$P_e \leqslant \epsilon \text{ and } R_e = \frac{1}{n} H(\boldsymbol{S}|\boldsymbol{Z}) \geqslant R_s - \epsilon. \tag{6}$$

During a given transmission frame, the delay limited SC C_s is the maximum achievable rate R_s that satisfies (6).

Encoder Construction: In order to transmit the message index $s \in \{1, 2, \ldots, 2^{nR_s}\}$ we map s to a set of indices $\{s_m\}$, $m = 1, \ldots, M$, by dividing the nR_s bits which correspond to the message index into a set of $\{NR_s^{(m)}\}$ bits with $\sum_{m=1}^{M} R_s^{(m)} = R_s$ and using a power allocation policy $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_M)$ so that a frame-based power constraint is satisfied,

$$\sum_{m=1}^{M} \gamma_m \leq MP, \text{ and } \gamma_m \geq 0 \text{ for } m = 1, \ldots, M. \tag{7}$$

1) Full CSI Feedback: Assuming that during the m-th block the full CSI (α_m, β_m) is fedback to the transmitter, then for each γ_m we can develop a sequence of $(2^{NR_s^{(m)}}, N)$ Gaussian codes using a pair of corresponding encoding and decoding functions (φ_m, ϕ_m) with $\varphi_m : \mathcal{S}^{q_m} \to \mathcal{X}_m^N$, $\phi_m : \mathcal{Y}_m^N \to \mathcal{S}^{q_m}$ and $\sum_{m=1}^{M} q_m = q$, that achieve the m-th block SC given by

$$c_s^{(full)}(\alpha_m, \beta_m, \gamma_m) = \left(\log \frac{1 + \alpha_m \gamma_m(\alpha_m, \beta_m)}{1 + \beta_m \gamma_m(\alpha_m, \beta_m)} \right)^+, \tag{8}$$

such that the m-th block probability of error

$$P_e^{(m)} = \Pr\left(\phi_m(\boldsymbol{y}_m \neq \boldsymbol{s}_m)\right) \to 0, \text{ as } N \to \infty. \tag{9}$$

Using the above multiplexing strategy, the probability of decoding error in a frame is upper bounded by

$$P_e \leq \sum_{m=0}^{M-1} P_e^{(m)} \to 0 \tag{10}$$

for finite M. As a consequence, for any power policy $\boldsymbol{\gamma}$ satisfying the power constraint (7) the secrecy rate $R_s^{(full)}$ is achievable:

$$R_s^{(full)}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}(\boldsymbol{\alpha}, \boldsymbol{\beta})) = \frac{1}{M} \sum_{m=0}^{M-1} c_s^{(full)}(\alpha_m, \beta_m, \gamma_m(\alpha_m, \beta_m)). \tag{11}$$

The delay limited SC $C_s^{(full)}$ of the outlined scheme is the maximum rate when the optimal power policy is used:

$$C_s^{(full)}(\boldsymbol{\alpha}, \boldsymbol{\beta}) \doteq \max_{\boldsymbol{\gamma}(\boldsymbol{\alpha}, \boldsymbol{\beta})} R_s^{(full)}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}(\boldsymbol{\alpha}, \boldsymbol{\beta})), \text{ s.t. (7)}. \tag{12}$$

2) Absence of CSI Feedback: In the absence of CSI feedback (blind scenario), for a power allocation γ_m we define the random variable:

$$R_s^{(bl)}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}) = \frac{1}{M} \sum_{m=0}^{M-1} \left(\log \frac{1 + \alpha_m \gamma_m}{1 + \beta_m \gamma_m} \right)^+. \tag{13}$$

Our objective is to solve the maximization problem

$$\max_{\boldsymbol{\gamma}} \mathbb{E}_{\boldsymbol{\alpha}, \boldsymbol{\beta}} \left[R_s^{(bl)}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}) \right], \text{ s.t. (7)}. \tag{14}$$

B. Secrecy Outage Probability

Let the power policy $\boldsymbol{\gamma}$ satisfy (7). The probability of secrecy outage (PSO) with respect to a target secrecy rate τ is given by

$$\begin{cases} P_{out}^{(full)}(\boldsymbol{\gamma}(\boldsymbol{\alpha},\boldsymbol{\beta}),\tau) \doteq Pr\big(R_s^{(full)} < \tau\big), & \text{full CSI} \\ P_{out}^{(bl)}(\boldsymbol{\gamma},\tau) \doteq Pr\big(R_s^{(bl)} < \tau\big). & \text{blind} \end{cases} \tag{15}$$

We note that the quantities (11) and (13) are continuous increasing concave functions of γ, therefore instead of solving the minimization of (15), which are non-convex problems, we solve problem (12) for the full CSI case, and problem (14) for the blind case, which are convex problems.

III. Dynamic Programming Formulation of the Optimal Power Allocation

Regarding the formulation of the constrained optimization problems that describe the optimal power allocation in BF-AWGN channels, there are three options regarding the timeline of events:

1) *Blind scenario*: no CSI information is available when the decision on the power allocation is made.
2) *Acausal full CSI scenario*: the full M-block CSI is available at the beginning of the transmission frame.
3) *Casual full CSI scenario*: the m-th block CSI is fedback to the transmitter before the decision on the m-th block power allocation is made but no future CSI is available.

We investigate cases 1) and 3) using DP while case 2) has been solved in [25] as a convex optimization problem leading to the secure waterfilling algorithm.

In further detail, the maximization problems (12) and (14) can be written as stochastic dynamic programs as follows: We define the stages $m = 1,\dots,M$, of the DP to be the transmission blocks. We let the state of the DP be the remaining power p_m at stage m and the decisions of the DP to be the power used at the current block m, γ_m. We denote by $V_m(p_m)$ (called the value function) the expected value of the secrecy rate gained from block m to the end of the horizon if the optimal power allocation policy is used.

Then, in the blind scenario the DP is written as:

$$\begin{aligned} &V_m(p_m) = \\ &\max_{0\le\gamma_m\le p_m} \mathbb{E}_{\alpha_m,\beta_m}\left[\left(\log\frac{1+\alpha_m\gamma_m}{1+\beta_m\gamma_m}\right)^+ + V_{m+1}(p_m-\gamma_m)\right] \\ &V_M(p_M) = 0. \end{aligned} \tag{16}$$

In the blind scenario the action space is simply $\gamma_m \in [0, p_m]$.

On the other hand, in the causal scenario we define an extended action space $\mathbb{A}_m$ that incorporates a check on the positiveness of the SC of the m-th block. We define $\delta_m = \alpha_m - \beta_m$. The SC of the block m is non-zero as long as $\mathbb{1}_{\{\delta_m>0\}} = 1$, where $\mathbb{1}_{\{\cdot\}}$ denotes the indicator function. Then, the DP is written as:

$$\begin{aligned} V_m(p_m) &= \max_{\gamma_m\in\mathbb{A}_m}\left(\log\frac{1+\alpha_m\gamma_m}{1+\beta_m\gamma_m}\right)^+ \\ &+ \mathbb{E}_{\alpha_{m+1},\beta_{m+1}}\left[V_{m+1}(p_m-\gamma_m)\right] \\ \mathbb{A}_m &= \left\{\gamma_m : 0\le\gamma_m\le p_m\mathbb{1}_{\{\delta_m>0\}}\right\} \\ V_M(p_M) &= 0. \end{aligned} \tag{17}$$

In the sequel we derive an analytic solution to (16) but not to (17). Even though the DP in (17) can be approximated computationally using appropriate discretization of the state, control space and outcome space of the random channels, we resort to approximate solutions that we can obtain in closed form. The closed form sub-optimal power allocations can be calculated in negligible computational time that is well suited for real-time applications with delay constraints of less than $1-5$ msec, for example in 5G networks. If we let D be the number of discrete values that we use to discretize the power region and we let W be the number of discrete values we use to discretize the outcome space of the random channels α and β, then the complexity of numerically evaluating the DP is proportional to MD^2W^2. Even though this is polynomial in these parameters, it is still not fast enough for real-time implementation, especially if large values of D and W are used to ensure a good approximation of the discretization.

IV. Optimal Power Control in the Blind Scenario

We assume a power constraint over M blocks in the form of (7). 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. We first consider the case in which we take a decision on the value of $\boldsymbol{\gamma}$ without having information on the CSI $(\boldsymbol{\alpha},\boldsymbol{\beta})$. In this formulation, our objective is to solve (14). As we will see, this formulation is equivalent to the quasi-static case with $M = 1$, perfect CSI at the receiver and no CSI at the transmitter.

Proposition 1: The problem described in (14) is solved by the power allocation policy $\boldsymbol{\gamma}' = (\gamma_1',\dots,\gamma_M')$ that corresponds to equidistribution of the available power, i.e.,

$$\gamma_m' = P, m = 1,\dots,M. \tag{18}$$

Proof: See Appendix A.

We note that in delay unconstrained applications, i.e. for $M\to\infty$, the secrecy rate

$$\frac{1}{M}\sum_{m=0}^{M-1}\mathbb{E}_{\alpha_m,\beta_m}\left[\left(\log\frac{1+\alpha_m P}{1+\beta_m P}\right)^+\right] \tag{19}$$

is achievable as the codewords can be multiplexed over all channel realizations in the ergodic setting; this rate corresponds to the ergodic SC with only receiver CSI. On the other hand, for finite M, it is not guaranteed that this secrecy rate can be achieved; albeit, the optimal transmission strategy with respect to objective (14) is still the equidistribution of the available power.

The above result agrees with intuition; as expected, due to symmetry the blind maximization of a function of the outcomes of M independent trials can be achieved by equally allocating the resources. An upper bound for the minimum PSO for a target secrecy rate τ and a frame based power constraint as in (7) can derived by using the blind policy and

can be expressed as:

$$\begin{aligned}\min_{\boldsymbol{\gamma}} P_{out}^{(bl)}(\boldsymbol{\gamma},\tau) &\leq P_{out}^{(bl)}(P,\tau)\\ &= Pr\left(\frac{1}{M}\sum_{m=1}^{M}\left(\log\frac{1+\alpha_m P}{1+\beta_m P}\right)^{+}<\tau\right)\\ &= Pr\left(\left(\log\frac{1+\alpha P}{1+\beta P}\right)^{+}<\tau\right),\end{aligned} \tag{20}$$

where the generic random variables α,β have the same underlying pdf as the random variables $\alpha_m,\beta_m, m=1,\ldots,M$. When no CSI is fedback to the transmitter, the PSO of the BF-AWGN channel reduces to the PSO of a quasi-static channel with $M=1$. As a result, in the blind case the frequency or the time diversity (expressed through $M>1$) does not translate into any gain in terms of PSO, in contrary to the full CSI case as will be demonstrated in sections V-VI.

Assuming a Rayleigh scattering environment, then α,β follow exponential distributions with pdfs expressed as:

$$f_\alpha(\alpha)=\frac{1}{\mu_\alpha}e^{-\frac{\alpha}{\mu_\alpha}}, f_\beta(\beta)=\frac{1}{\mu_\beta}e^{-\frac{\beta}{\mu_\beta}}, \tag{21}$$

and corresponding cumulative distribution functions (cdf)

$$F_\alpha(\alpha)=1-e^{-\frac{\alpha}{\mu_\alpha}}, F_\beta(\beta)=1-e^{-\frac{\beta}{\mu_\beta}}, \tag{22}$$

with mean values μ_α and μ_β respectively. Notably, in [5] the negative result that the PSO of quasi-static Rayleigh channels is bounded away from 0 even for diminishing secrecy rates $\tau\to 0$ was obtained and the PSO was expressed as:

$$P_{out}^{(bl)}(P,\tau)\Big|_{\tau\to 0}=\frac{\mu_\beta}{\mu_\alpha+\mu_\beta}. \tag{23}$$

Naturally, in statistically equivalent fading conditions with $\mu_\alpha=\mu_\beta$ half of the transmission blocks will most likely be in a secrecy outage, even for diminishing target secrecy rates.

However, in the following we will show that this negative effect can be overcome in networks with receiver diversity of orders K and E for the legitimate user and the eavesdropper respectively, as long as $K>E$. Receiver diversity of orders K and E can occur either by using K and E receive antennas at the legitimate user and the eavesdropper, respectively, or through a max SNR channel allocation policy in a network with K legitimate terminals and E malicious nodes. To simplify some of the mathematical derivations we further assume that statistical equivalence holds with $\mu_\alpha=\mu_\beta=1$ and that we are in the high SNR regime, i.e., $P\gg 1$.

Considering diversity orders K and E, the channel gain of the legitimate user α and of the eavesdropper β correspond to the K-th and E-th order statistic, respectively, of $f_\alpha(\alpha)$ and $f_\beta(\beta)$. In the absence of cooperation, the distributions $f_K^{(K)}(\alpha)$ of $\alpha=\max_{k\in\{1,\ldots,K\}}(\alpha_k)$ and $f_E^{(E)}(\beta)$ of $\beta=\max_{j\in\{1,\ldots,E\}}(\beta_j)$ are then given by

$$f_K^{(K)}(\alpha) = KF_\alpha(\alpha)^{K-1}f_\alpha(\alpha), \tag{24}$$

$$f_E^{(E)}(\beta) = EF_\beta(\beta)^{E-1}f_\beta(\beta). \tag{25}$$

On the other hand, if the full diversity is exploited and the optimal maximum ratio combiner (MRC) receivers are employed, then the distributions $f^{(K)}(\alpha)$ of $\alpha=\sum_{k=1}^{K}\alpha_k$ and $f^{(E)}(\beta)$ of $\beta=\sum_{j=1}^{E}\beta_k$ can be expressed as [26]:

$$f^{(K)}(\alpha)=\frac{K\alpha^{K-1}e^{-\alpha}}{(K-1)!}, f^{(E)}(\beta)=\frac{E\beta^{E-1}e^{-\beta}}{(E-1)!}. \tag{26}$$

Finally, in the high SNR regime, i.e., for $P\gg 1$, the following limits hold:

$$\lim_{P\to\infty}\left(\log\frac{1+\alpha P}{1+\beta P}\right)^{+}=\left(\log\frac{\alpha}{\beta}\right)^{+}, \tag{27}$$

$$\lim_{P\to\infty}\left(\log\frac{1+\sum_{k=1}^{K}\alpha_k P}{1+\sum_{j=1}^{E}\beta_i P}\right)^{+}=\left(\log\frac{\sum_{k=1}^{K}\alpha_k}{\sum_{j=1}^{E}\beta_j}\right)^{+}. \tag{28}$$

From (25) and (27) the minimum PSO w.r.t. a target transmission rate τ in the non-cooperative case can be upper bounded by

$$\begin{aligned}P_{out}^{(bl,nc)}(K,E,\tau) &= 1-\int_0^\infty K(1-e^{-x})^{K-1}e^{-x}\\ &\quad\int_0^{x2^{-\tau}} E(1-e^{-y})^{E-1}e^{-y}\mathrm{d}y\mathrm{d}x\\ &= K\Gamma(K)\sum_{n=1}^{E}(-1)^{n+1}\binom{E}{n}\frac{\Gamma(n2^{-\tau}+1)}{\Gamma(K+n2^{-\tau}+1)}\end{aligned} \tag{29}$$

For diminishing $\tau\to 0$ (29) simplifies to:

$$P_{out}^{(bl,nc)}\Big|_{\tau\to 0}=\frac{E}{K+E}. \tag{30}$$

Furthermore, from (26) and (28) the minimum PSO with full diversity can on the other hand be upper bounded by

$$\begin{aligned}P_{out}^{(bl,co)}(K,E,\tau) &= 1-\int_0^\infty\frac{Kx^{K-1}e^{-x}}{(K-1)!}\\ &\quad\int_0^{x2^{-\tau}}\frac{Ey^{E-1}e^{-y}}{(E-1)!}\mathrm{d}y\mathrm{d}x\\ &= 1-\frac{\sum_{n=0}^{K-1}\binom{K+E-1}{n}2^{n\tau}}{(1+2^\tau)^{K+E-1}}.\end{aligned} \tag{31}$$

For $\tau\to 0$ and using $\sum_{n=0}^{k}\binom{k}{n}=2^k$, the PSO with full diversity can be expressed as

$$P_{out}^{(bl,co)}\Big|_{\tau\to 0} = \frac{\sum_{n=K}^{K+E-1}\binom{K+E-1}{n}}{2^{K+E-1}} \tag{32}$$

$$\leq \frac{\binom{K+E-1}{K}}{2^K}, \tag{33}$$

where for the derivation of the bound (33) we have used that $\sum_{k=q}^{n}\binom{n}{k}\binom{k}{q}=2^{n-q}\binom{n}{q}$ and that $\binom{n}{q}\leq\binom{n}{k}\binom{k}{q}$ for $n\geq q$. The asymptotic expressions for the PSO in (30) and (33) demonstrate the dramatic impact of diversity in the feasibility of secrecy in *statistically equivalent* Rayleigh channels. Notably, the exponential decay of the asymptotic PSO in the fully cooperative case underlines the potential for exploiting PLS techniques in networks in which the intended destinations have large diversity orders, e.g. cooperative sensor networks or massive single input multiple output (SIMO) systems. On the other hand, these same expressions highlight the limitations of PLS approaches in coordinated attacks from multiple eavesdroppers.

V. Optimal Power Control with Acausal Full 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 [25]. It is repeated below for completeness as it will be used for comparison in the numerical experiments. This is the baseline secure waterfilling policy and its performance cannot be exceeded in the causal or blind scenario.

Proposition 2: Without loss of generality we assume that the pairs of channel gains (α_m, β_m), $m = 1, \ldots, M$ are already permuted so that the differences

$$\delta_m = \alpha_m - \beta_m \tag{34}$$

appear in non-increasing order. We further define the inverse channel gaps d_m as:

$$d_m = \frac{1}{\beta_m} - \frac{1}{\alpha_m}. \tag{35}$$

The power allocation $\boldsymbol{\gamma}^* = (\gamma_0^*, \ldots, \gamma_{M-1}^*)$ that achieves the acausal BF-AWGN SC

$$C_s^{(full)}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \frac{1}{M} \sum_{m=1}^{M} \left(\log \frac{1 + \alpha_m \gamma_m^*}{1 + \beta_m \gamma_m^*} \right)^+ \tag{36}$$

and satisfies the M-block power constraint (7) with equality is given by the secure waterfilling algorithm:

$$\gamma_m^*\left(\frac{1}{\lambda}\right) = \frac{1}{2}\left[\sqrt{d_m^2 + \frac{4}{\lambda} d_m} - \left(\frac{2}{\alpha_m} + d_m\right)\right] \cdot \mathbb{1}_{\{m \in \mathbb{Q}\}} \tag{37}$$

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

Proof: See [25].

The functions $\gamma_m^*(\lambda^{-1})$ are monotone increasing and continuous in λ^{-1}. As a result, there exists a unique integer μ in $\{1, \ldots, M\}$ 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., $\sum_{m=0}^{\mu} \gamma_m^*(\lambda^{-1}) = MP$.

Finally, in this case the minimum PSO is a deterministic step function with threshold τ:

$$\min_{\boldsymbol{\gamma}} P_{out}^{(full)}(\boldsymbol{\gamma}, \tau) = \mathbb{1}_{\left\{C_s^{(full)}(\boldsymbol{\alpha}, \boldsymbol{\beta}) < \tau\right\}} \tag{38}$$

VI. Near-Optimal Power Control with Causal Full 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 optimization problem given in (17). Unlike the blind case, we were not able to find analytic solutions to (17). Further, as discussed in section III, instead of numerically evaluating the DP, we resort to approximation methods that provide us with closed form solutions, which are evaluated in negligible computational times. We will find near-optimal solutions to the problem in (17) in three different cases; in the low SNR regime, in the high SNR regime and finally using a universal approximation that incorporates the blind scenario policy.

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 m-th block SC given by:

$$c_s^{(full)}(\alpha_m, \beta_m, \gamma_m) \simeq (\alpha_m - \beta_m)^+ \gamma_m = (\delta_m)^+ \gamma_m, \tag{39}$$

with δ_m defined in (34). Using the above approximation and substituting into the optimality equations (17) for the last two frames $m = M$ and $m = M - 1$ we get $\gamma_M^{(th)} = p_M \mathbb{1}_{\{\delta_M > 0\}}$ and $\gamma_{M-1}^{(th)} = p_{M-1} \mathbb{1}_{\{(\delta_{M-1})^+ > \mathbb{E}[(\delta)^+]\}}$. Motivated by the power allocation of the last two frames we propose the following approximation:

Low SNR Approximation: In the low SNR regime, i.e, for $P \ll 1$, we approximate the solution to problem (17) by the "threshold power allocation" $\boldsymbol{\gamma}^{(th)} = (\gamma_1^{(th)}, \ldots, \gamma_M^{(th)})$ with

$$\gamma_m^{(th)} = p_m \mathbb{1}_{\{(\delta_m)^+ > \mathbb{E}[(\delta)^+]\}} \tag{40}$$

with $p_1 = MP$ and $m = 1, \ldots, M$. Using the threshold policy, the SC in the low SNR regime can be approximated by

$$C_s^{(full,lo)} \simeq (\delta_{m^*})^+ MP \tag{41}$$

with m^* denoting the smallest index $m^* \in \{1, \ldots, M\}$ that satisfies $(\delta_{m^*})^+ > \mathbb{E}\left[(\delta_{m^*})^+\right]$. 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 MP. Intuitively, in the low SNR regime there will not be many opportunities for achieving high values of the per block SC, so whenever such an opportunity occurs it should be seized.

Next, turning our attention to the case in which a minimum secrecy rate τ should also be achieved, then the transmission threshold needs to be set to $\frac{\tau}{MP}$. At the end of the horizon the PSO is a deterministic step function with threshold τ:

$$P_{out}^{(full,lo)}(\tau) = \mathbb{1}_{\left\{C_s^{(full,lo)} < \tau\right\}} \tag{42}$$

To evaluate the PSO at the beginning of the horizon, let us denote by p the probability that during the m-th transmission block the threshold $\frac{\tau}{MP}$ is not reached:

$$Pr\left((\delta_m)^+ < \frac{\tau}{MP}\right) = p. \tag{43}$$

As a result, the PSO at the beginning of the horizon with causal CSI in the low SNR regime can be expressed as:

$$P_{out}^{(full,lo)}(\tau) = p^M. \tag{44}$$

We note that even when the legitimate user's channel is on average worse than the eavesdropper's, it can still be possible to transmit at some non-zero rate 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 $P \gg 1$, we can transmit at very high power during any of the transmission blocks. A good approximation for the SC during the m-th block is derived as

$$\lim_{\gamma\to\infty} c_s^{(full)}(\alpha_m,\beta_m,\gamma_m) = \left(\log\frac{\alpha_m}{\beta_m}\right)^+. \quad (45)$$

The SC is as a result independent of the power allocation and any transmission policy $\gamma_m \in \mathbb{A}_m$ could be used. We propose the use of a high power allocation policy as below:
High SNR Approximation: In the high SNR regime, i.e, for $P \gg 1$, the solution to problem (17) can be approximated by the "high power allocation" $\boldsymbol{\gamma}^{(hi)} = (\gamma_1^{(hi)},\ldots,\gamma_M^{(hi)})$ with

$$\gamma_m^{(hi)} = \frac{p_m}{M-m}\mathbb{1}_{\{\delta_m>0\}} \quad (46)$$

with $p_1 = MP$ and $m = 1,\ldots,M$. The SC can be approximated by

$$C_s^{(full,hi)} \simeq \frac{1}{M}\sum_{m=1}^{M}\left(\log\frac{\alpha_m}{\beta_m}\right)^+. \quad (47)$$

At the end of the horizon, the PSO is a deterministic step function with threshold τ:

$$P_{out}^{(full,hi)}(\tau) = \mathbb{1}_{\left\{C_s^{(full,hi)}<\tau\right\}}. \quad (48)$$

On the other hand, at the beginning of the horizon the SC is the sum of M i.i.d. random variables. Using the central limit theorem and denoting by μ and σ^2 the mean value and the variance of the per block SC, the M-block BF-AWGN channel SC can be approximated by a Gaussian random variable with mean value μ and variance $\frac{\sigma^2}{M}$. As a result, at the beginning of the horizon the PSO can be expressed as:

$$\begin{aligned} P_{out}^{(full,hi)}(\tau) &= Pr\left(C_s^{(full,hi)}<\tau\right) \\ &= \int_0^\tau \frac{\sqrt{M}}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{M(x-\mu)^2}{2\sigma^2}\right)\mathrm{d}x \\ &= \frac{1}{2}\mathrm{erf}\left(\sqrt{\frac{M}{2\sigma^2}}\mu\right) - \frac{1}{2}\mathrm{erf}\left(\sqrt{\frac{M}{2\sigma^2}}(\mu-\tau)\right). \end{aligned} \quad (49)$$

As M increases the variance of the PSO at the beginning of the horizon decreases. In the limiting case of the ergodic channel, i.e., for $M\to\infty$, the SC converges to μ and the PSO becomes a step function with threshold μ.

C. Blind Horizon Approximation (BHA)

In this subsection 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 expressed in (17). We use the approximation

$$\begin{aligned} &\mathbb{E}_{\alpha_{m+1},\beta_{m+1}}\left[V_{m+1}(p_m-\gamma_m)\right] \\ &\qquad \simeq (M-m)c_s^{(full)}\left(\mu_\alpha,\mu_\beta,\frac{p_m-\gamma_m}{M-m}\right), \end{aligned} \quad (50)$$

where μ_α and μ_β are the expected values of the channel gains of the legitimate user and the eavesdropper respectively. The proposed approximation for the horizon of future events reduces future values of the channel gains to their expected values; as a result, in the future the optimal power allocation is the equidistribution of the resources and (50) follows straightforwardly. We note in passing that due to Jensen's inequality and the concavity of the function V_{m+1} the proposed approximation overestimates the return of the value function in the horizon of future events leading to a conservative strategy for the present.
BHA Approximation: The solution to problem (17) can be approximated by the "blind horizon approximation (BHA) power allocation" $\boldsymbol{\gamma}^{(bha)} = (\gamma_1^{(bha)},\ldots,\gamma_M^{(bha)})$ with

$$\gamma_m^{(bha)} = \begin{cases} \varrho_m, & \text{if } \alpha_m>\beta_m \text{ and } \mu_\alpha>\mu_\beta, \\ \gamma_m^{(th)} & \text{if } \alpha_m>\beta_m \text{ and } \mu_\alpha\le\mu_\beta, \\ 0, & \text{otherwise,} \end{cases} \quad (51)$$

where $\varrho_m = \left(\min(x_2^{(m)},p_m)\right)^+$ and $x_2^{(m)}$ is the second root of

$$\begin{aligned} &\frac{\mathrm{d}}{\mathrm{d}\gamma_m}\Big\{c_s^{(full)}(\alpha_m,\beta_m,\gamma_m) \\ &\qquad + \quad (M-m)c_s^{(full)}\big(\mu_\alpha,\mu_\beta,\frac{p_m-\gamma_m}{M-m}\big)\Big\} = 0. \end{aligned}$$

Derivation of BHA policy: See Appendix B.

VII. Numerical results

A. No CSI Feedback

In this subsection we present results for the PSO in the blind scenario. In Figs. 1 and 2 the PSOs (29) and (31) for a target secrecy rate $\tau = 1$ bit/sec/Hz are depicted. Similarly to the asymptotic PSO in (30) and (33) for diminishing $\tau\to 0$, the effect of cooperation proves a decisive factor in identifying an operational region in which a secrecy outage occurs with very high probability and a region in which the PSO is negligible. In particular, as shown in Fig. 2, when exploiting the full diversity the network exhibits a phase transition characteristic in terms of secrecy.

Furthermore, in Fig. 3 we plot the minimum required number of diversity order K versus the diversity order E in order to ensure the secret transmission of $\tau = \{0.1,1,2\}$ bit/sec/Hz with a 99% certainty, i.e., for $P_{out}^{(bl,co)}(K,E,\tau) < 0.01$. Notably, in the presence of a single eavesdropper without diversity ($E=1$), this can be achieved when the intended destination has a diversity order $K = \{6,11,20\}$ respectively.

B. Full CSI Feedback

In this subsection, we present numerical evaluations of the average secrecy rates when various transmission policies are adopted in Nakagami-m channels. The channel gains α_m and β_m follow a Gamma distribution

$$f_{\mathcal{X}}(x) = \frac{1}{\Gamma(m)\theta^m}x^{m-1}e^{-\frac{x}{\theta}} \quad (52)$$

with mean value $\mu = m\theta$. For $m=1$ the Nakagami-m channel is equivalent to a Rayleigh channel while for $m\to\infty$

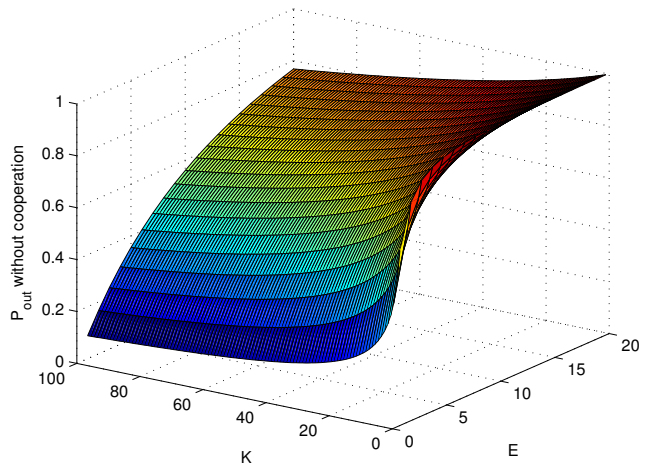

Fig. 1. PSO for the blind policy in the non-cooperative case for $\tau = 1$ bit/sec/Hz and diversity orders K and E.

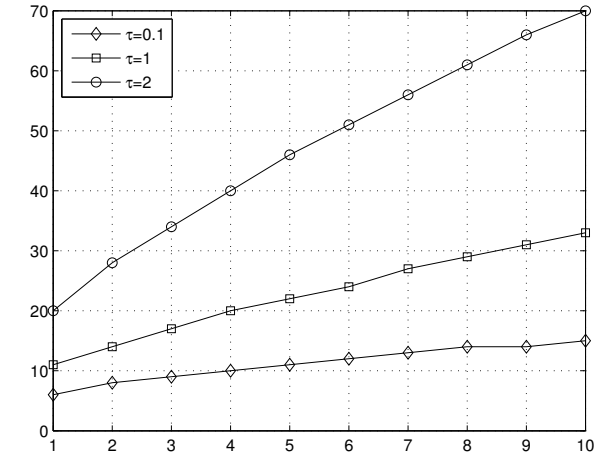

Fig. 3. Minimum K required to transmit $0.1, 1$ and 2 bit/sec/Hz with $P_{out}^{(bl,co)'} < 0.01$ as a function of E.

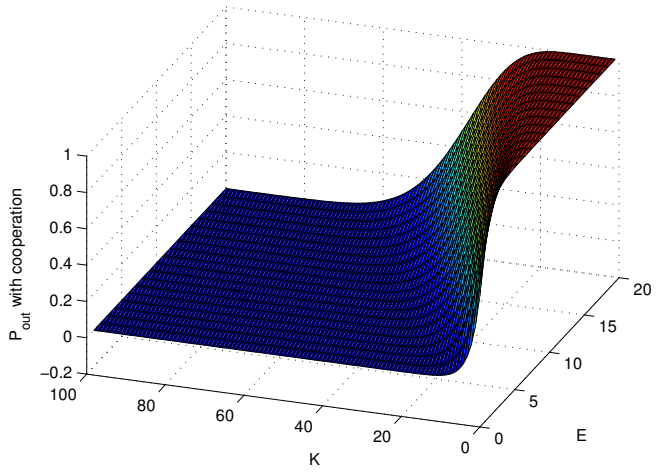

Fig. 2. PSO for the blind policy in the cooperative case for $\tau = 1$ bit/sec/Hz and diversity orders K and E.

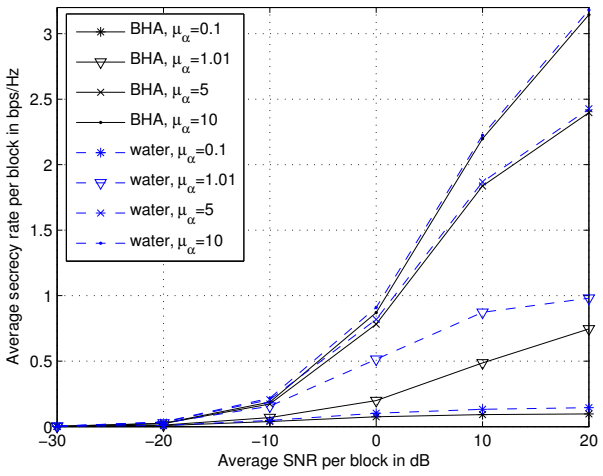

Fig. 4. Average secrecy rates achieved with causal BHA policy and acausal waterfilling policy for various policies for $\mu_\beta = 1$ and $M = 10$.

it is equivalent to an AWGN channel. In Fig. 4 the average secrecy rates per block achieved by the causal BHA policy and the acausal waterfilling are depicted for Rayleigh scattering with $m = 1$, $\mu_\beta = 1$ and $M = 10$. The average legitimate user SNR is set to $\mu_\alpha P$ and the results are averaged over 1000 channel realizations. Interestingly, as long as μ_α is distinctively 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.

In the second set of simulations we compare the average secrecy rates achieved by the various transmission policies, normalized to the secure waterfilling SC for Nakagami-m channels with $m = 1, 2$. We set $M = 10, \mu_\beta = 1$ and the average legitimate user SNR to $\mu_\alpha P$. In Figs. 5 and 6 we depict the secrecy rates for $\mu_\alpha = 0.1, 1.01, 5$, averaged over 1000 channel realizations. We note that the waterfilling rate is not achievable in the case of causal CSI. It can be seen that the threshold policy outperforms the high power policy in the low SNRs and vice versa in the high SNRs. Furthermore, the high power policy always outperforms the blind policy as in the latter part of the power budget is spent on blocks with zero SC when $\alpha_m < \beta_m$. On the other hand, for $\mu_\alpha \leq \mu_\beta$ the BHA policy coincides with the threshold policy. In this case the BHA policy is not optimal in all SNR and is outperformed in the intermediate and high SNR regimes by the high power 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 high power policy over the entire SNR axis.

Furthermore, in Fig. 7 the effect of the horizon length is investigated. We plot the acausal SC and average secrecy rates for the BHA and the blind policies for Nakagami-m channels with $m = 1, 2, 10$, block SNR set to 10 dB and various block lengths. It can be concluded that for $M > 10$, the various al-

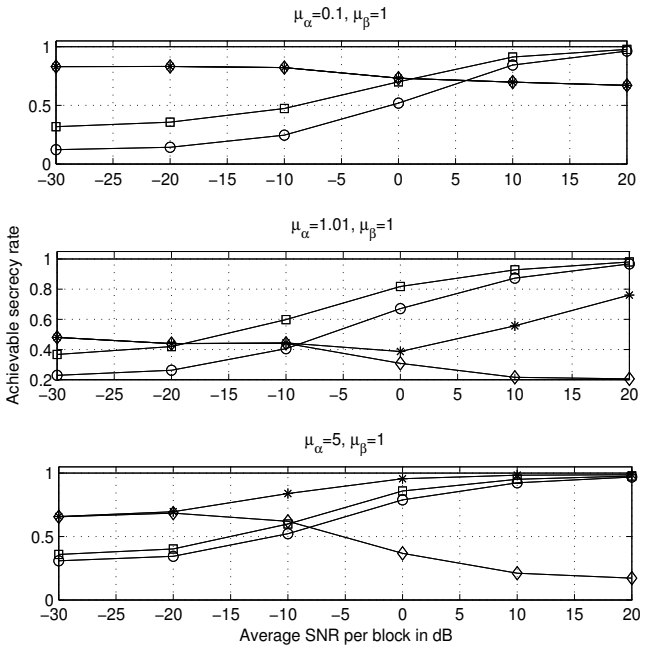

Fig. 5. Average secrecy rates of Nakagami-1 channels normalized to the acausal waterfilling rate achieved with various policies and $\mu_\beta = 1$, $M = 10$, $\diamond$: threshold policy, $\square$: high power policy, o: blind policy, *: BHA policy

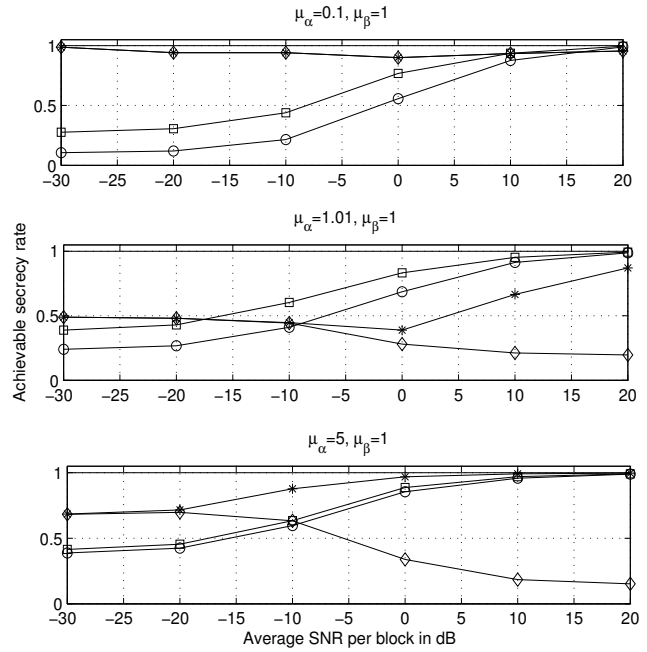

Fig. 6. Average secrecy rates of Nakagami-2 channels normalized to the acausal waterfilling policy achieved with various policies and $\mu_\beta = 1$, $M = 10$, $\diamond$: threshold policy, $\square$: high power policy, o: blind policy, *: BHA policy

gorithms converge to their asymptotic values which have been evaluated for the ergodic scenario as $\{1.3016, 1.1792, 1.0066\}$ bps/Hz, respectively. Notably for $m = 1, 2$ the asymptotic values and the ergodic values coincide, while for $m = 10$, we

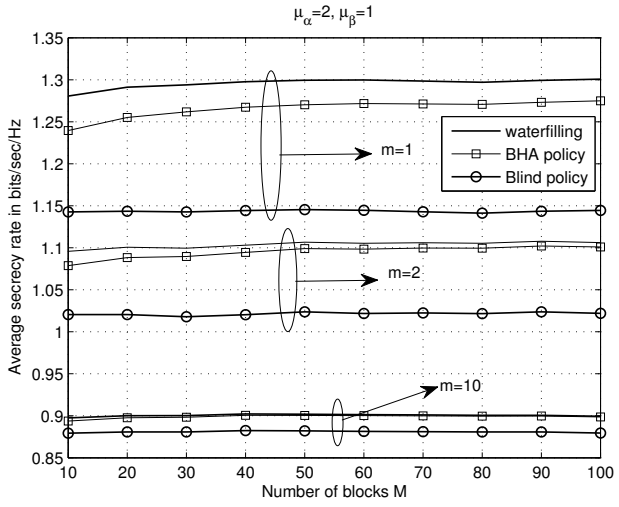

Fig. 7. Secrecy rates achieved with the blind policy, the causal BHA policy and the acausal waterfilling for Nakagami channels with $m = 1, 2, 10$ and block SNR=10 dB.

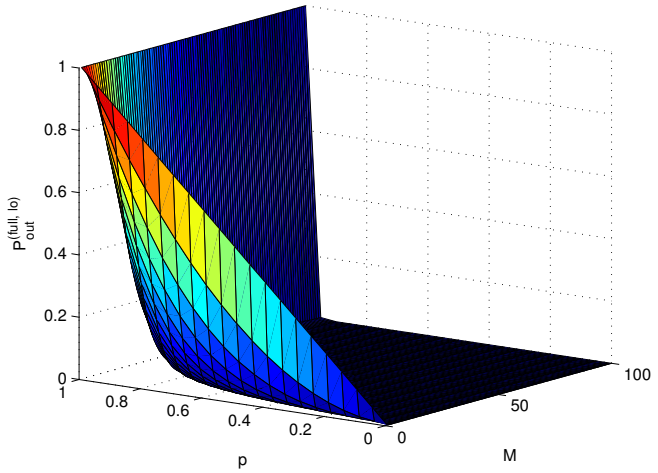

Fig. 8. PSO at the beginning of the horizon with causal CSI in the low SNR regime.

observe a small gap indicating a very slow convergence as M increases. Furthermore, the lack of a line of sight component (LOS) in the Rayleigh channel increases the M-block SC compared to channels with LOS (i.e., for $m = 2$) or that are closer to an AWGN channel (for $m = 10$). The increasing variance of Nakagami-m channels with decreasing m results in a larger "variability" in the channel coefficients that can provide notable gains in terms of secrecy when compared to AWGN channels.

Finally, in Figs. 8 and 9 we depict the PSO at the beginning of the horizon in the causal CSI scenario in the low and the high SNR regimes. The PSO in the high SNR regime is evaluated at $M = 10$ and expected value $\mu = 2$ and variance $\sigma^2 = 1$ for the per block SC. In both cases it is possible to determine regions with negligible PSO values and design the wireless network accordingly.

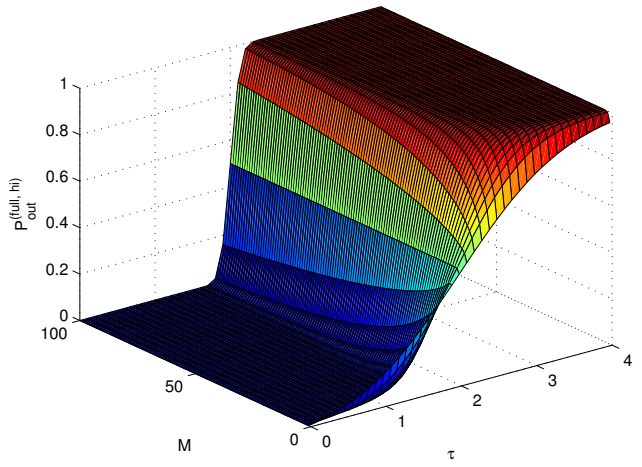

Fig. 9. PSO at the beginning of the horizon with causal CSI in the high SNR regime.

VIII. Conclusions

In the present work we have investigated the optimal power allocation in delay constrained M-block BF-AWGN 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. Remarkably, it has been demonstrated that in a fully cooperative network the PSO decays exponentially fast in Rayleigh channels with the diversity order of the legitimate user for small secrecy rates. The PSO in the general case exhibits a phase transition that allows to identify an operational region in which the transmission of secret messages with a very high probability is guaranteed even in absence of CSI feedback. As an example, with full diversity of order 11 in the presence of an eavesdropper without diversity it is possible to transmit 1 bit/sec/Hz with perfect secrecy in 99% of the transmission blocks.

Furthermore, we have outlined the benchmark secure waterfilling algorithm that achieves the M-block BF-AWGN channel SC when the full CSI is acausally available to the transmitter. Next, 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 derived a near optimal threshold policy whereas in the high SNR regime a high power 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 for Nakagami-m channels 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 high power transmission policies as long as the mean legitimate user's SNR is greater than the mean eavesdropper's SNR.

Future extensions of this work will include semi-blind scenarios in which only the legitimate user CSI is fedback to the transmitter.

Appendix

A. Proof of Proposition 1

Let $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_M)$. Due to the stationarity of the BF-AWGN channel, the stochastic optimization objective function can be written as follows:

$$\max_{\boldsymbol{\gamma}} \mathbb{E}_{\boldsymbol{\alpha},\boldsymbol{\beta}} \left[R_s^{(bl)} \right] = \max_{\gamma} \mathbb{E}_{\alpha,\beta} \left[\left(\frac{1+\alpha\gamma}{1+\beta\gamma} \right)^+ \right] \tag{53}$$

where the expectation is written with rapport to the generic random variables α and β. We define the function:

$$f(\gamma) \equiv \mathbb{E}_{\alpha,\beta} \left[\log \left(\frac{1+\alpha\gamma}{1+\beta\gamma} \right)^+ \right]. \tag{54}$$

Then, the problem in (53) can be written as a stochastic DP as follows: We let $V_m(p_m)$ be the expected value of the secrecy rate gained from block m to the end of the horizon if the optimal power allocation policy is used. Then the DP equations can be written as:

$$\begin{aligned} V_m(p_m) &= \max_{0 \le \gamma_m \le p_m} f(\gamma_m) + V_{m+1}(p_m - \gamma_m) \\ &\quad \text{for } m = 1, \ldots, M-1 \\ V_M(p_M) &= 0. \end{aligned} \tag{55}$$

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

$$\left.\frac{\mathrm{d}g_m}{\mathrm{d}\gamma}\right|_{\gamma=0} = \frac{[\mu_\alpha\mu_\beta L_m^2(\alpha_m - \beta_m)]p_m^2 + [L_m(\alpha_m - \beta_m)(\mu_\alpha + \mu_\beta)]p_m + [(\alpha_m - \beta_m) - (\mu_\alpha - \mu_\beta)]}{(1 + \mu_\alpha L_m p_m)(1 + \mu_\beta L_m p_m)}$$

$$\left.\frac{\mathrm{d}g_m}{\mathrm{d}\gamma}\right|_{\gamma=p_m} = \frac{[-\alpha_m\beta_m(\mu_\alpha - \mu_\beta)]p_m^2 + [-(\mu_\alpha - \mu_\beta)(\alpha_m + \beta_m)]p_m + [(\alpha_m - \beta_m) - (\mu_\alpha - \mu_\beta)]}{(1 + \alpha_m p_m)(1 + \beta_m p_m)}$$

We perform backward DP on the optimality equations (55). We start the recursion at block $m = M$, where the optimality equations are:

$$V_M(p_M) = \max_{0 \le \gamma_M \le p_M} f(\gamma_M), \tag{56}$$

Since f is nondecreasing, the maximization in (56) 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:

$$V_{M-1}(p_{M-1}) = \max_{0 \le \gamma_{M-1} \le p_{M-1}} f(\gamma_{M-1}) + f(p_{M-1} - \gamma_{M-1}). \tag{57}$$

Let $h(\gamma) = f(\gamma) + f(p-\gamma)$. Note that $\frac{\mathrm{d}h(\gamma)}{\mathrm{d}\gamma} = \frac{\mathrm{d}f(\gamma)}{\mathrm{d}\gamma} - \frac{\mathrm{d}f(p-\gamma)}{\mathrm{d}\gamma}$, and since $\frac{\mathrm{d}f(\gamma)}{\mathrm{d}\gamma}$ is nonincreasing and $\frac{\mathrm{d}f(p-\gamma)}{\mathrm{d}\gamma}$ is nondecreasing in γ, we have that $\frac{\mathrm{d}h(\gamma)}{\mathrm{d}\gamma}$ is nonincreasing. This means that it can have at most one extreme point in the interval $[0, p_{M-1}]$, and the extreme point must be a maximum. At $\gamma = \frac{p_{M-1}}{2}$ we have: $\frac{\mathrm{d}h(\gamma)}{\mathrm{d}\gamma}|_{\gamma = p_{M-1}/2} = 0$. Therefore in (57) 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

$$V_{M-n}(p_{M-n}) = (n+1) f\Big(\frac{p_{M-n}}{n+1}\Big) \tag{58}$$

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 $m = 1, \ldots, M$ $\gamma'_m = P$.

B. Derivation of the BHA Approximation

The proposed approximation for V_m is given as:

$$\hat{V}_m(p_m) = \max_{\gamma_m \in \mathbb{A}_m} g_m(\gamma_m), \tag{59}$$

where g_m is as follows:

$$g_m(\gamma) = c_s^{(full)}(\alpha_m, \beta_m, \gamma) + (M-m) c_s^{(full)}\left(\mu_\alpha, \mu_\beta, \frac{p_m - \gamma}{M-m}\right), \tag{60}$$

1) 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:

$$g_m(\gamma) = \log\left(\frac{1+\alpha_m\gamma}{1+\beta_m\gamma}\right) + (M-m)\log\left(\frac{1+\mu_\alpha\frac{p_m-\gamma}{M-m}}{1+\mu_\beta\frac{p_m-\gamma}{M-m}}\right). \tag{61}$$

Taking $\frac{\mathrm{d}g_m(\gamma)}{\mathrm{d}\gamma} = 0$ gives the following roots:

$$(x_1^{(m)}, x_2^{(m)}) = \left(\frac{E_m + \sqrt{G_m}}{2F_m}, \frac{E_m - \sqrt{G_m}}{2F_m}\right) \tag{62}$$

where E_m, F_m are given below and G_m is given at the bottom of the previous page. For simplicity of notation we let $L_m = \frac{1}{M-m}$:

$$\begin{aligned} E_m &= 2\mu_\alpha\mu_\beta L_m^2(\alpha_m - \beta_m)p_m + [L_m(\alpha_m - \beta_m) \\ &\times (\mu_\alpha + \mu_\beta) + (\alpha_m + \beta_m)(\mu_\alpha - \mu_\beta)], \\ F_m &= \mu_\alpha\mu_\beta L_m^2(\alpha_m - \beta_m) - \alpha_m\beta_m(\mu_\alpha - \mu_\beta), \end{aligned}$$

When $\alpha_m > \beta_m$ and $\mu_\alpha > \mu_\beta$, $G_m \ge 0$.

To prove that $x_1^{(m)}$ is always outside the interval $[0, p_m]$, we have two cases, according to the sign of F_m: for $F_m > 0$, $x_1^{(m)} \ge \frac{E_m}{2F_m} > p_m$, while for $F_m < 0$, $x_1^{(m)} < 0$.

Regarding whether $x_2^{(m)}$ is in the interval $[0, p_m]$ we first calculate the derivative of g_m at points 0 and p_m, given at the bottom of the previous page. If $(\alpha_m - \beta_m) \ge (\mu_\alpha - \mu_\beta)$, then $\frac{\mathrm{d}g_m}{\mathrm{d}\gamma}\big|_{\gamma=0} \ge 0$. Since only one root of $\frac{\mathrm{d}g_m}{\mathrm{d}\gamma}$ can exist in the interval $[0, p_m]$, then the root (the maximum) must be outside of the interval $[0, p_m]$, $x_2^{(m)} \ge p_m$, and the maximum is achieved at p_m. However, if $\frac{\mathrm{d}g_m}{\mathrm{d}\gamma} < 0$ 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 $\min(x_2^{(m)}, p_m)$. If on the other hand $(\alpha_m - \beta_m) < (\mu_\alpha - \mu_\beta)$, then $\frac{\mathrm{d}g_m}{\mathrm{d}\gamma} \le 0$. Since only one root of $\frac{\mathrm{d}g_m}{\mathrm{d}\gamma}$ can exist in the interval $[0, p_m]$, then the root (the maximum) must be outside of the interval $[0, p_m]$, $x_2^{(m)} \le 0$ and the maximum is achieved at 0. However, if $\frac{\mathrm{d}g_m}{\mathrm{d}\gamma} > 0$ then the root must be in $[0, p_m]$ and the maximum is achieved at $x_2^{(m)}$. Thus the maximum in $[0, p_m]$ is achieved at $\max(0, x_2^{(m)})$. This gives the power allocation in (51).

2) Case II: $\alpha_m > \beta_m$ and $\mu_\alpha < \mu_\beta$: When $\alpha_m > \beta_m$ and $\mu_\alpha < \mu_\beta$ the function g_m can be rewritten as:

$$g_m(\gamma) = \log\left(\frac{1+\alpha_m\gamma}{1+\beta_m\gamma}\right) \tag{63}$$

and the BHA reduces to the threshold policy so that $\gamma_m^{(bha)} = p_m$.

3) Case III: $\alpha_m < \beta_m$: When $\alpha_m < \beta_m$ the function g_m can be rewritten as:

$$g_m(\gamma) = (M-m)\log\left(\frac{1+\mu_\alpha\frac{p_m-\gamma}{M-m}}{1+\mu_\beta\frac{p_m-\gamma}{M-m}}\right) \tag{64}$$

and the optimal BHA policy is to allocate no power, i.e., $\gamma_m^{(bha)} = 0$.

REFERENCES

[1] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*. Hanover, MA: Now Publishers, 2009.

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

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[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] 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.

[8] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Trans. Information Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[9] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Information Theory*, vol. 57, no. 8, pp. 4961 – 4972, Aug. 2011.

[10] X. Tang, R. Liu, P. Spasojevic, and H.V. Poor, "Interference assisted secret communication," *IEEE Trans. Information Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[11] A. Chorti, "Helping interferer physical layer security strategies for M-QAM and M-PSK systems," in *46th Annual Conference on Information Sciences and Systems (CISS)*, Princeton NJ, USA, Mar. 2012, pp. 1–6.

[12] 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, pp. 1850–1863, Sep. 2013.

[13] D. Lun, Z. Han, A. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays (part 2)," *IEEE Trans. Signal Processing*, vol. 58, no. 3, pp. 1845–1888, Mar. 2010.

[14] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 1, pp. 388–396, Feb. 2012.

[15] A. Chorti, M. M. Molu, D. Karpuk, C. Hollanti, and A. Burr, "Strong secrecy in wireless network coding systems with M-QAM modulators," *arXiv:1407.0915v1 [cs.CR]*, Jul. 2014, to be presented to ICCC'14.

[16] 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.

[17] 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.

[18] 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.

[19] A. Goldsmith and M. Medard, "Capacity of time-varying channels with causal channel side information," *IEEE Trans. Information Theory*, vol. 53, no. 3, pp. 881 – 899, Mar. 2007.

[20] M. Kobayashi, P. Piantanida, S. Yang, and S. Shamai (Shitz), "On the secrecy degrees of freedom of the multiantenna block fading wiretap channels," *IEEE Trans. on Information Forensics and Security*, vol. 6, no. 11, pp. 703–711, Sep. 2011.

[21] T. Koike-Akino, A. F. Molisch, C. Duan, Z. Tao, and P. Orlik, "Capacity, mse and secrecy analysis of linear block precoding for distributed antenna systems in multi-user frequency-selective fading channels," *IEEE Trans. on Communications*, vol. 59, no. 3, pp. 888–900, Mar. 2011.

[22] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Information Theory*, vol. 59, no. 9, pp. 5379–5397, Sep. 2013.

[23] Z. Rezki, A. Khisti, and M.-S. Alouini, "Ergodic secret message capacity of the wiretap channel with finite-rate feedback," *IEEE Trans. on Wireless Communications*, vol. 13, no. 6, pp. 3364–3379, Jun. 2014.

[24] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. NY: Cambridge University Press, Sep. 2011.

[25] 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.

[26] H.-C. Yang and M.-S. Alouini, *Diversity, Adaptation and Sceduling in MIMO and OFDM Systems*. Cambridge, UK: Cambridge University Press, 2011.