

Secure Communication in the Low-SNR Regime: A Characterization of the Energy-Secrecy Tradeoff

Mustafa Cenk Gursoy

Department of Electrical Engineering

University of Nebraska-Lincoln, Lincoln, NE 68588

Email: gursoy@engr.unl.edu

Abstract—¹ Secrecy capacity of a multiple-antenna wiretap channel is studied in the low signal-to-noise ratio (SNR) regime. Expressions for the first and second derivatives of the secrecy capacity with respect to SNR at SNR = 0 are derived. Transmission strategies required to achieve these derivatives are identified. In particular, it is shown that it is optimal in the low-SNR regime to transmit in the maximum-eigenvalue eigenspace of $\Phi = \mathbf{H}_m^\dagger \mathbf{H}_m - \frac{N_m}{N_e} \mathbf{H}_e^\dagger \mathbf{H}_e$ where \mathbf{H}_m and \mathbf{H}_e denote the channel matrices associated with the legitimate receiver and eavesdropper, respectively, and N_m and N_e are the noise variances at the receiver and eavesdropper, respectively. Energy efficiency is analyzed by finding the minimum bit energy required for secure and reliable communications, and the wideband slope. Increased bit energy requirements under secrecy constraints are quantified. Finally, the impact of fading is investigated.

I. INTRODUCTION

Secure transmission of confidential messages is a critical issue in communication systems and especially in wireless systems due to the broadcast nature of wireless transmissions. In [1], Wyner addressed the transmission security from an information-theoretic point of view, and identified the rate-equivocation region and established the secrecy capacity of the discrete memoryless wiretap channel in which the wiretapper receives a degraded version of the signal observed by the legitimate receiver. The secrecy capacity is defined as the maximum communication rate from the transmitter to the legitimate receiver, which can be achieved while keeping the eavesdropper completely ignorant of the transmitted messages. Later, these results are extended to Gaussian wiretap channel in [2]. In [3], Csiszár and Körner considered a more general wiretap channel model and established the secrecy capacity when the transmitter has a common message for two receivers and a confidential message to only one. Recently, there has been a flurry of activity in the area of information-theoretic security, where, for instance, the impact of fading, cooperation, and interference on secrecy are studied (see e.g., [4] and the articles and references therein). Several recent results also addressed the secrecy capacity when multiple-antennas are employed by the transmitter, receiver, and the eavesdropper [5]–[9]. The secrecy capacity for the most general case in which arbitrary number of antennas are present at each terminal has been established in [8] and [9].

In addition to security issues, another pivotal concern in most wireless systems is energy-efficient operation especially when wireless units are powered by batteries. From an information-theoretic perspective, energy efficiency can be measured by the energy required to send one information bit reliably. It is well-known that for unfaded and fading Gaussian channels subject

to average input power constraints, energy efficiency improves as one operates at lower SNR levels, and the minimum bit energy is achieved as SNR vanishes [11]. Hence, requirements on energy efficiency necessitate operation in the low-SNR regime. Additionally, operating at low SNR levels has its benefits in terms of limiting the interference in wireless systems.

In this paper, in order to address the two critical issues of security and energy-efficiency jointly, we study the secrecy capacity in the low-SNR regime. We consider a general multiple-input and multiple-output (MIMO) channel model and identify the optimal transmission strategies in this regime under secrecy constraints. Since secrecy capacity is in general smaller than the capacity attained in the absence of confidentiality concerns, energy per bit requirements increase due to secrecy constraints. In this work, we quantify these increased energy costs and address the energy-secrecy tradeoff.

II. CHANNEL MODEL

We consider a MIMO channel model and assume that the transmitter, legitimate receiver, and eavesdropper are equipped with n_T , n_R , and n_E antennas, respectively. We further assume that the channel input-output relations between the transmitter and legitimate receiver, and the transmitter and eavesdropper are given by

$$\mathbf{y}_m = \mathbf{H}_m \mathbf{x} + \mathbf{n}_m \quad \text{and} \quad \mathbf{y}_e = \mathbf{H}_e \mathbf{x} + \mathbf{n}_e, \quad (1)$$

respectively. Above, \mathbf{x} denotes the $n_T \times 1$ -dimensional transmitted signal vector. This channel input is subject to the following average power constraint:

$$\mathbb{E}\{\|\mathbf{x}\|^2\} = \text{tr}(\mathbf{K}_x) \leq P \quad (2)$$

where tr denotes the trace operation and $\mathbf{K}_x = E\{\mathbf{x}\mathbf{x}^\dagger\}$ is the covariance matrix of the input. In (1), $n_R \times 1$ -dimensional \mathbf{y}_m and $n_E \times 1$ -dimensional \mathbf{y}_e represent the received signal vectors at the legitimate receiver and eavesdropper, respectively. Moreover, \mathbf{n}_m with dimension $n_R \times 1$ and \mathbf{n}_e with dimension $n_E \times 1$ are independent, zero-mean Gaussian random vectors with $E\{\mathbf{n}_m \mathbf{n}_m^\dagger\} = N_m \mathbf{I}$ and $E\{\mathbf{n}_e \mathbf{n}_e^\dagger\} = N_e \mathbf{I}$, where \mathbf{I} is the identity matrix. The signal-to-noise ratio is defined as

$$\text{SNR} = \frac{\mathbb{E}\{\|\mathbf{x}\|^2\}}{\mathbb{E}\{\|\mathbf{n}_m\|^2\}} = \frac{P}{n_R N_m}. \quad (3)$$

Finally, in the channel models, \mathbf{H}_m is the $n_R \times n_T$ -dimensional channel matrix between the transmitter and legitimate receiver, and \mathbf{H}_e is the $n_E \times n_T$ -dimensional channel matrix between the transmitter and eavesdropper. While being fixed deterministic

¹This work was supported in part by the NSF CAREER Grant CCF-0546384. 978-1-4244-4313-0/09/\$25.00 ©2009 IEEE

matrices in unfaded channels, \mathbf{H}_m and \mathbf{H}_e in fading channels are random matrices whose components denote the fading coefficients between the corresponding antennas at the transmitting and receiving ends.

III. SECRECY IN THE LOW-SNR REGIME

Recently, in [8] and [9], it has been shown that when the channel matrices \mathbf{H}_m and \mathbf{H}_e are fixed for the entire transmission period and are known to all three terminals, then the secrecy capacity in nats per dimension is given by²

$$C_s = \frac{1}{n_R} \max_{\substack{\mathbf{K}_x \succeq \mathbf{0} \\ \text{tr}(\mathbf{K}_x) \leq P}} \log \det \left(\mathbf{I} + \frac{1}{N_m} \mathbf{H}_m \mathbf{K}_x \mathbf{H}_m^\dagger \right) - \log \det \left(\mathbf{I} + \frac{1}{N_e} \mathbf{H}_e \mathbf{K}_x \mathbf{H}_e^\dagger \right) \quad (4)$$

where the maximization is over all possible input covariance matrices $\mathbf{K}_x \succeq \mathbf{0}^3$ subject to a trace constraint. We note that since $\log \det \left(\mathbf{I} + \frac{1}{N_m} \mathbf{H}_m \mathbf{K}_x \mathbf{H}_m^\dagger \right)$ is a concave function of \mathbf{K}_x , the objective function in (4) is in general neither concave nor convex in \mathbf{K}_x , making the identification the optimal input covariance matrix a difficult task.

In this paper, we concentrate on the low-SNR regime. In this regime, the behavior of the secrecy capacity can be accurately predicted by its first and second derivatives with respect to SNR at SNR = 0:

$$C_s(\text{SNR}) = \dot{C}_s(0)\text{SNR} + \frac{\ddot{C}_s(0)}{2}\text{SNR}^2 + o(\text{SNR}^2). \quad (5)$$

Moreover, $\dot{C}_s(0)$ and $\ddot{C}_s(0)$ also enable us to analyze the energy efficiency in the low-SNR regime through [11]

$$\frac{E_b}{N_{0,s,\min}} = \frac{\log 2}{\dot{C}_s(0)} \text{ and } \mathcal{S}_0 = \frac{2 \left[\dot{C}_s(0) \right]^2}{-\ddot{C}_s(0)} \quad (6)$$

where $\frac{E_b}{N_{0,s,\min}}$ denotes the minimum bit energy required for reliable communication under secrecy constraints, and \mathcal{S}_0 denotes the wideband slope which is the slope of the secrecy capacity in bits/dimension/(3 dB) at the point $\frac{E_b}{N_{0,s,\min}}$. These quantities provide a linear approximation of the secrecy capacity in the low-SNR regime. While $\frac{E_b}{N_{0,s,\min}}$ is a performance measure for vanishing SNR, \mathcal{S}_0 together with $\frac{E_b}{N_{0,s,\min}}$ characterize the performance at low but nonzero SNRs. We note that the formula for the minimum bit energy is valid if C_s is a concave function of SNR, which we show later in the paper.

The following result identifies the first and second derivatives of the secrecy capacity at SNR = 0.

Theorem 1: The first derivative of the secrecy capacity in (4) with respect to SNR at SNR = 0 is

$$\dot{C}_s(0) = [\lambda_{\max}(\Phi)]^+ = \begin{cases} \lambda_{\max}(\Phi) & \text{if } \lambda_{\max}(\Phi) > 0 \\ 0 & \text{else} \end{cases} \quad (7)$$

where $\Phi = \mathbf{H}_m^\dagger \mathbf{H}_m - \frac{N_m}{N_e} \mathbf{H}_e^\dagger \mathbf{H}_e$. Moreover, the second deriva-

tive of the secrecy capacity at SNR = 0 is given by

$$\ddot{C}_s(0) = -n_R \min_{\substack{\{\alpha_i\} \\ \alpha_i \in [0,1] \forall i \\ \sum_{i=1}^l \alpha_i = 1}} \sum_{i,j=1}^l \alpha_i \alpha_j \left(|\mathbf{u}_j^\dagger \mathbf{H}_m^\dagger \mathbf{H}_m \mathbf{u}_i|^2 - \frac{N_m^2}{N_e^2} |\mathbf{u}_j^\dagger \mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{u}_i|^2 \right) 1_{\{\lambda_{\max}(\Phi) > 0\}} \quad (8)$$

where l is the multiplicity of $\lambda_{\max}(\Phi) > 0$, $\{\mathbf{u}_i\}$ are the eigenvectors that span the maximum-eigenvalue eigenspace, and $1_{\{\lambda_{\max}(\Phi) > 0\}} = \begin{cases} 1 & \text{if } \lambda_{\max}(\Phi) > 0 \\ 0 & \text{else} \end{cases}$ is the indicator function.

Proof: We first note that the input covariance matrix $\mathbf{K}_x = E\{\mathbf{x}\mathbf{x}^\dagger\}$ is by definition a positive semidefinite Hermitian matrix. As a Hermitian matrix, \mathbf{K}_x can be written as [13, Theorem 4.1.5]

$$\mathbf{K}_x = \mathbf{U} \mathbf{\Lambda} \mathbf{U}^\dagger \quad (9)$$

where \mathbf{U} is a unitary matrix and $\mathbf{\Lambda}$ is a real diagonal matrix. Using (9), we can also express \mathbf{K}_x as

$$\mathbf{K}_x = \sum_{i=1}^{n_T} d_i \mathbf{u}_i \mathbf{u}_i^\dagger \quad (10)$$

where $\{d_i\}$ are the diagonal components of $\mathbf{\Lambda}$, and $\{\mathbf{u}_i\}$ are the column vectors of \mathbf{U} and form an orthonormal set. Assuming that the input uses all the available power, we have $\text{tr}(\mathbf{K}_x) = \sum_{i=1}^{n_T} d_i = P$. Noting that \mathbf{K}_x is positive semidefinite and hence $d_i \geq 0$, we can write $d_i = \alpha_i P$ where $\alpha_i \in [0, 1] \forall i$ and $\sum_{i=1}^{n_T} \alpha_i = 1$. Now, the secrecy rate achieved with a particular covariance matrix \mathbf{K}_x can be expressed as

$$I_s(\text{SNR}) = \frac{1}{n_R} \left(\log \det \left(\mathbf{I} + n_R \text{SNR} \sum_{i=1}^{n_T} \alpha_i \mathbf{H}_m \mathbf{u}_i \mathbf{u}_i^\dagger \mathbf{H}_m^\dagger \right) - \log \det \left(\mathbf{I} + \frac{n_R N_m}{N_e} \text{SNR} \sum_{i=1}^{n_T} \alpha_i \mathbf{H}_e \mathbf{u}_i \mathbf{u}_i^\dagger \mathbf{H}_e^\dagger \right) \right). \quad (11)$$

where SNR is defined in (3). As also noted in [11], we can easily show that

$$\frac{d}{dv} \log \det(\mathbf{I} + v\mathbf{A})|_{v=0} = \text{tr}(\mathbf{A}), \quad (12)$$

$$\frac{d^2}{dv^2} \log \det(\mathbf{I} + v\mathbf{A})|_{v=0} = -\text{tr}(\mathbf{A}^2). \quad (13)$$

Now, using (12), we obtain the following expression for the first derivative of the secrecy rate I_s with respect to SNR at SNR = 0:

$$\dot{I}_s(0) = \sum_{i=1}^{n_T} \alpha_i \left(\text{tr}(\mathbf{H}_m \mathbf{u}_i \mathbf{u}_i^\dagger \mathbf{H}_m^\dagger) - \frac{N_m}{N_e} \text{tr}(\mathbf{H}_e \mathbf{u}_i \mathbf{u}_i^\dagger \mathbf{H}_e^\dagger) \right) \quad (14)$$

$$= \sum_{i=1}^{n_T} \alpha_i \left(\mathbf{u}_i^\dagger \mathbf{H}_m^\dagger \mathbf{H}_m \mathbf{u}_i - \frac{N_m}{N_e} \mathbf{u}_i^\dagger \mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{u}_i \right) \quad (15)$$

$$= \sum_{i=1}^{n_T} \alpha_i \mathbf{u}_i^\dagger \left(\mathbf{H}_m^\dagger \mathbf{H}_m - \frac{N_m}{N_e} \mathbf{H}_e^\dagger \mathbf{H}_e \right) \mathbf{u}_i = \sum_{i=1}^{n_T} \alpha_i \mathbf{u}_i^\dagger \Phi \mathbf{u}_i \quad (16)$$

where (15) follows from the property that $\text{tr}(\mathbf{A}\mathbf{B}) = \text{tr}(\mathbf{B}\mathbf{A})$. Also, in (16), we have defined $\Phi = \mathbf{H}_m^\dagger \mathbf{H}_m - \frac{N_m}{N_e} \mathbf{H}_e^\dagger \mathbf{H}_e$. Since Φ is a Hermitian matrix and $\{\mathbf{u}_i\}$ are unit vectors, we have [13,

²Unless stated otherwise, all logarithms throughout the paper are to the base e .

³ \succeq and \succ denote positive semidefinite and positive definite partial orderings, respectively, for Hermitian matrices. If $\mathbf{A} \succeq \mathbf{B}$, then $\mathbf{A} - \mathbf{B}$ is a positive semidefinite matrix. Similarly, $\mathbf{A} \succ \mathbf{B}$ implies that $\mathbf{A} - \mathbf{B}$ is positive definite.

Theorem 4.2.2]

$$\mathbf{u}_i^\dagger \Phi \mathbf{u}_i \leq \lambda_{\max}(\Phi) \quad \forall i \quad (17)$$

where $\lambda_{\max}(\Phi)$ denotes the maximum eigenvalue of the matrix Φ . Recall that $\alpha_i \in [0, 1]$ and $\sum_i \alpha_i = 1$. Then, from (17), we obtain

$$\dot{I}_s(0) = \sum_{i=1}^{n_T} \alpha_i \mathbf{u}_i^\dagger \Phi \mathbf{u}_i \leq \lambda_{\max}(\Phi). \quad (18)$$

Note that this upper bound can be achieved if, for instance, $\alpha_1 = 1$ and $\alpha_i = 0 \quad \forall i \neq 1$, and \mathbf{u}_1 is chosen as the eigenvector that corresponds to the maximum eigenvalue of Φ . Heretofore, we have implicitly assumed that $\lambda_{\max}(\Phi) > 0$ and all the available power is used to transmit the information in the direction of the maximum eigenvalue. If $\lambda_{\max}(\Phi) \leq 0$, then all eigenvalues of Φ are less than or equal to zero, and hence Φ is a negative semidefinite matrix. In this situation, none of the channels of the legitimate receiver is stronger than those corresponding ones of the eavesdropper. In such a case, secrecy capacity is zero. Therefore, if $\lambda_{\max}(\Phi) \leq 0$, we have $\dot{C}_s(0) = 0$. Finally, we conclude from (18) and the above discussion that the first derivative of the secrecy capacity with respect to SNR at SNR = 0 is given by

$$\dot{C}_s(0) = [\lambda_{\max}(\Phi)]^+ = \begin{cases} \lambda_{\max}(\Phi) & \text{if } \lambda_{\max}(\Phi) > 0 \\ 0 & \text{else} \end{cases}. \quad (19)$$

If $\lambda_{\max}(\Phi) > 0$ is distinct, $\dot{C}_s(0)$ is achieved when we choose $\mathbf{K}_x = P \mathbf{u}_1 \mathbf{u}_1^\dagger$ where \mathbf{u}_1 is the eigenvector that corresponds to $\lambda_{\max}(\Phi)$. Therefore, beamforming in the direction in which the eigenvalue of Φ is maximized is optimal in the sense of achieving the first derivative of the secrecy capacity in the low-SNR regime. More generally, if $\lambda_{\max}(\Phi) > 0$ has a multiplicity, any covariance matrix in the following form achieves the first derivative:

$$\mathbf{K}_x = P \sum_{i=1}^l \alpha_i \mathbf{u}_i \mathbf{u}_i^\dagger \quad (20)$$

where l is the multiplicity of the maximum eigenvalue, $\{\mathbf{u}_i\}_{i=1}^l$ are the eigenvectors that span the maximum-eigenvalue eigenspace, and $\{\alpha_i\}_{i=1}^l$ are constants, taking values in $[0, 1]$ and having the sum $\sum_{i=1}^l \alpha_i = 1$. Therefore, transmission in the maximum-eigenvalue eigenspace is necessary to achieve $\dot{C}_s(0)$.

Next, we consider the second derivative of the secrecy capacity. Again, when $\lambda_{\max}(\Phi) \leq 0$, the secrecy capacity is zero and therefore $\ddot{C}_s(0) = 0$. Hence, in the following, we consider the case in which $\lambda_{\max}(\Phi) > 0$. Suppose that the input covariance matrix is chosen as in (20) with a particular set of $\{\alpha_i\}$. Then, using (13), we can obtain

$$\begin{aligned} \ddot{I}_s(0) &= -n_R \operatorname{tr} \left(\left(\sum_{i=1}^l \alpha_i \mathbf{H}_m \mathbf{u}_i \mathbf{u}_i^\dagger \mathbf{H}_m^\dagger \right)^2 \right) \\ &\quad + n_R \frac{N_m^2}{N_e^2} \operatorname{tr} \left(\left(\sum_{i=1}^l \alpha_i \mathbf{H}_e \mathbf{u}_i \mathbf{u}_i^\dagger \mathbf{H}_e^\dagger \right)^2 \right) \\ &= -n_R \sum_{i,j} \alpha_i \alpha_j \left(|\mathbf{u}_j^\dagger \mathbf{H}_m^\dagger \mathbf{H}_m \mathbf{u}_i|^2 - \frac{N_m^2}{N_e^2} |\mathbf{u}_j^\dagger \mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{u}_i|^2 \right) \end{aligned} \quad (21)$$

$$(22)$$

where (22) is obtained by using the fact that $\operatorname{tr}(\mathbf{A}\mathbf{B}) = \operatorname{tr}(\mathbf{B}\mathbf{A})$ and performing some straightforward manipulations. Note again that $\{\mathbf{u}_i\}$ are the eigenvectors spanning the maximum-eigenvalue eigenspace of Φ . Being necessary to achieve the first derivative, the covariance structure given in (20) is also necessary to achieve the second derivative. Therefore, the second derivative of the secrecy capacity at SNR = 0 is the maximum of the expression in (22) over all possible values of $\{\alpha_i\}$. Hence,

$$\ddot{C}_s(0) = -n_R \min_{\substack{\{\alpha_i\} \\ \alpha_i \in [0,1] \forall i \\ \sum_{i=1}^l \alpha_i = 1}} \sum_{i,j} \alpha_i \alpha_j \left(|\mathbf{u}_j^\dagger \mathbf{H}_m^\dagger \mathbf{H}_m \mathbf{u}_i|^2 - \frac{N_m^2}{N_e^2} |\mathbf{u}_j^\dagger \mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{u}_i|^2 \right) \quad (23)$$

Since $\ddot{C}_s(0)$ is equal to the expression in (23) when $\lambda_{\max}(\Phi) > 0$ and is zero otherwise, the final expression in (8) is obtained by multiplying the formula in (23) with the indicator function $1\{\lambda_{\max}(\Phi) > 0\}$. ■

Remark 1: In the absence of secrecy constraints, the first and second derivatives of the MIMO capacity at SNR = 0 are [11]

$$\dot{C}(0) = \lambda_{\max}(\mathbf{H}_m^\dagger \mathbf{H}_m) \quad \text{and} \quad \ddot{C}(0) = -\frac{n_R}{l} \lambda_{\max}^2(\mathbf{H}_m^\dagger \mathbf{H}_m) \quad (24)$$

where l is the multiplicity of $\lambda_{\max}(\mathbf{H}_m^\dagger \mathbf{H}_m)$. Hence, the first and second derivatives are achieved by transmitting in the maximum-eigenvalue eigenspace of $\mathbf{H}_m^\dagger \mathbf{H}_m$, the subspace in which the transmitter-receiver channel is the strongest. Due to the optimality of the water-filling power allocation method, power should be equally distributed in each orthogonal direction in this subspace in order for the second derivative to be achieved.

Remark 2: We see from Theorem 1 that when there are secrecy constraints, we should at low SNRs transmit in the direction in which the transmitter-receiver channel is strongest *with respect to the transmitter-eavesdropper channel* normalized by the ratio of the noise variances. For instance, $\dot{C}_s(0)$ can be achieved by beamforming in the direction in which the eigenvalue of Φ is maximized. On the other hand, if $\lambda_{\max}(\Phi)$ has a multiplicity, the optimization problem in (8) should be solved to identify how the power should be allocated to different orthogonal directions in the maximum-eigenvalue eigenspace so that the second-derivative $\ddot{C}_s(0)$ is attained. In general, the optimal power allocation strategy is neither water-filling nor beamforming. For instance, consider parallel Gaussian channels for both transmitter-receiver and transmitter-eavesdropper links, and assume that $\mathbf{H}_m^\dagger \mathbf{H}_m = \operatorname{diag}(5, 4, 2)$ and $\mathbf{H}_e^\dagger \mathbf{H}_e = \operatorname{diag}(2, 1, 1)$ where $\operatorname{diag}()$ is used to denote a diagonal matrix with components provided in between the parentheses. Assume further that the noise variances are equal, i.e., $N_m = N_e$. Then, it can be easily seen that $\lambda_{\max}(\Phi) = 3$ and has a multiplicity of 2. Solving the optimization problem in (8) provides $\alpha_1 = 5/12$ and $\alpha_2 = 7/12$. Hence, approximately, 42% of the power is allocated to the channel for which the transmitter-receiver link has a strength of 5, and 58% is allocated for the channel with strength 4.

Remark 3: When $\lambda_{\max}(\Phi) > 0$ is distinct, then beamforming in the direction in which $\lambda(\Phi)$ is maximized is optimal in the sense of achieving both $\dot{C}_s(0)$ and $\ddot{C}_s(0)$. Moreover, in this case,

we have

$$\ddot{C}_s(0) = -n_R \left(\|\mathbf{H}_m \mathbf{u}_1\|^4 - \frac{N_m^2}{N_e^2} \|\mathbf{H}_e \mathbf{u}_1\|^4 \right) \quad (25)$$

where \mathbf{u}_1 is the eigenvector that corresponds to $\lambda_{\max}(\Phi)$.

Remark 4: From [13, Theorem 4.3.1], we know that for two Hermitian matrices \mathbf{A} and \mathbf{B} with the same dimensions, we have

$$\lambda_{\max}(\mathbf{A} + \mathbf{B}) \leq \lambda_{\max}(\mathbf{A}) + \lambda_{\max}(\mathbf{B}). \quad (26)$$

Applying this result to our setting yields

$$\lambda_{\max}(\Phi) \leq \lambda_{\max}(\mathbf{H}_m^\dagger \mathbf{H}_m) - \lambda_{\min} \left(\frac{N_m}{N_e} \mathbf{H}_e^\dagger \mathbf{H}_e \right). \quad (27)$$

Therefore, we conclude from Remark 1 that secrecy constraints diminish the first derivative $\dot{C}_s(0)$ at least by a factor of $\lambda_{\min} \left(\frac{N_m}{N_e} \mathbf{H}_e^\dagger \mathbf{H}_e \right)$ when compared to the case in which there are no such constraints.

Remark 5: In the case in which each terminal has a single antenna, the results of Theorem 1 specialize to

$$\dot{C}_s(0) = \left[|h_m|^2 - \frac{N_m}{N_e} |h_e|^2 \right]^+ \quad (28)$$

$$\ddot{C}_s(0) = - \left[|h_m|^4 - \frac{N_m^2}{N_e^2} |h_e|^4 \right]^+. \quad (29)$$

In the next result, we show that the secrecy capacity is concave in SNR.

Proposition 1: The secrecy capacity C_s achieved under the average power constraint $\mathbb{E}\{\|\mathbf{x}\|^2\} \leq P$ is a concave function of SNR.

Proof: Concavity can be easily shown using the time-sharing argument. Assume that at power level P_1 and signal-to-noise ratio SNR_1 , the optimal input is \mathbf{x}_1 , which satisfies $\mathbb{E}\{\|\mathbf{x}_1\|^2\} \leq P_1$, and the secrecy capacity is $C_s(\text{SNR}_1)$. Similarly, for P_2 and SNR_2 , the optimal input is \mathbf{x}_2 , which satisfies $\mathbb{E}\{\|\mathbf{x}_2\|^2\} \leq P_2$, and the secrecy capacity is $C_s(\text{SNR}_2)$. Now, we assume that the transmitter performs time-sharing by transmitting at two different power levels using \mathbf{x}_1 and \mathbf{x}_2 . More specifically, in θ fraction of the time, the transmitter uses the input \mathbf{x}_1 , transmits at most at P_1 , and achieves the secrecy rate $C_s(\text{SNR}_1)$. In the remaining $(1-\theta)$ fraction of the time, the transmitter employs \mathbf{x}_2 , transmits at most at P_2 , and achieves the secrecy rate $C_s(\text{SNR}_2)$. Hence, this scheme overall achieves the average secrecy rate of

$$\theta C_s(\text{SNR}_1) + (1-\theta) C_s(\text{SNR}_2) \quad (30)$$

by transmitting at the level $\theta \mathbb{E}\{\|\mathbf{x}_1\|^2\} + (1-\theta) \mathbb{E}\{\|\mathbf{x}_2\|^2\} \leq P_\theta = \theta P_1 + (1-\theta) P_2$. The average signal-to-noise ratio is $\text{SNR}_\theta = \theta \text{SNR}_1 + (1-\theta) \text{SNR}_2$. Therefore, the secrecy rate in (30) is an achievable secrecy rate at SNR_θ . Since the secrecy capacity is the maximum achievable secrecy rate, the secrecy capacity at SNR_θ is larger than that in (30), i.e.,

$$C_s(\text{SNR}_\theta) = C_s(\theta \text{SNR}_1 + (1-\theta) \text{SNR}_2) \quad (31)$$

$$\geq \theta C_s(\text{SNR}_1) + (1-\theta) C_s(\text{SNR}_2), \quad (32)$$

showing the concavity. \blacksquare

We further note that the concavity can also be shown using the following facts. As also discussed in [10], MIMO secrecy capacity is obtained by proving in the converse argument that

the considered upper bound is tight and

$$C_s = \max_{p(\mathbf{x})} \min_{p(\mathbf{y}'_r, \mathbf{y}'_e | \mathbf{x}) \in \mathcal{D}} I(\mathbf{x}; \mathbf{y}'_r | \mathbf{y}'_e) \quad (33)$$

where \mathcal{D} is the set of joint conditional density functions $p(\mathbf{y}'_r, \mathbf{y}'_e | \mathbf{x})$ that satisfy $p(\mathbf{y}'_r | \mathbf{x}) = p(\mathbf{y}_r | \mathbf{x})$ and $p(\mathbf{y}'_e | \mathbf{x}) = p(\mathbf{y}_e | \mathbf{x})$. Note that for fixed channel distributions, the mutual information $I(\mathbf{x}; \mathbf{y}'_r | \mathbf{y}'_e)$ is a concave function of the input distribution $p(\mathbf{x})$. Since the pointwise infimum of a set of concave functions is concave [14], $f(p(\mathbf{x})) = \min_{p(\mathbf{y}'_r, \mathbf{y}'_e | \mathbf{x}) \in \mathcal{D}} I(\mathbf{x}; \mathbf{y}'_r | \mathbf{y}'_e)$ is also a concave function of $p(\mathbf{x})$. Concavity of the functional f and the fact that maximization is over input distributions satisfying $\mathbb{E}\{\|\mathbf{x}\|^2\} \leq P$ lead to the concavity of the secrecy capacity with respect to SNR.

We can now write the following corollary to Proposition 1 and Theorem 1.

Corollary 1: The minimum bit energy attained under secrecy constraints is

$$\frac{E_b}{N_{0,s,\min}} = \frac{\log 2}{[\lambda_{\max}(\Phi)]^+}. \quad (34)$$

Remark 6: From Remark 4, we can write

$$\begin{aligned} \frac{E_b}{N_{0,s,\min}} &= \frac{\log 2}{[\lambda_{\max}(\Phi)]^+} \geq \frac{\log 2}{\lambda_{\max}(\mathbf{H}_m^\dagger \mathbf{H}_m) - \lambda_{\min} \left(\frac{N_m}{N_e} \mathbf{H}_e^\dagger \mathbf{H}_e \right)} \\ &\geq \frac{\log 2}{\lambda_{\max}(\mathbf{H}_m^\dagger \mathbf{H}_m)} = \frac{E_b}{N_{0,\min}} \end{aligned} \quad (35)$$

where $\frac{E_b}{N_{0,\min}}$ in (35) denotes the minimum bit energy in the absence of secrecy constraints. Hence, in general, secrecy requirements increase the energy expenditure. When secure communication is not possible, $[\lambda_{\max}(\Phi)]^+ = 0$ and $\frac{E_b}{N_{0,s,\min}} = \infty$.

The expression for the wideband slope S_0 can be readily obtained by plugging in the expressions in (7) and (8) into that in (6).

Remark 7: Energy costs of secrecy can easily be identified in the single-antenna case. Clearly, the minimum bit energy in the presence of secrecy is strictly greater than that in the absence of such constraints:

$$\frac{E_b}{N_{0,s,\min}} = \frac{\log 2}{\left[|h_m|^2 - \frac{N_m}{N_e} |h_e|^2 \right]^+} > \frac{\log 2}{|h_m|^2} = \frac{E_b}{N_{0,\min}} \quad (36)$$

when $\frac{N_m}{N_e} |h_e|^2 > 0$. Furthermore, the energy requirement increases monotonically as the value of $\frac{N_m}{N_e} |h_e|^2$ increases. Indeed, when $\frac{N_m}{N_e} |h_e|^2 = |h_m|^2$, secure communication is not possible and $\frac{E_b}{N_{0,s,\min}} = \infty$.

IV. THE IMPACT OF FADING

In this section, we assume that the channel matrices \mathbf{H}_m and \mathbf{H}_e are random matrices whose components are ergodic random variables, modeling fading in wireless transmissions. We again assume that realizations of these matrices are perfectly known by all the terminals. As discussed in [12], fading channel can be regarded as a set of parallel subchannels each of which corresponds to a particular fading realization. Hence, in each subchannel, the channel matrices are fixed similarly as in the channel model considered in the previous section. In [12], Liang *et al.* have shown that having independent inputs for each

subchannel is optimal and the secrecy capacity of the set of parallel subchannels is equal to the sum of the capacities of subchannels. Therefore, the secrecy capacity of fading channels can be found by averaging the secrecy capacities attained for different fading realizations.

We assume that the transmitter is subject to a short-term power constraint. Hence, for each channel realization, the same amount of power is used and we have $\text{tr}(\mathbf{K}_x) \leq P$. With this assumption, the transmitter is allowed to perform power adaptation in space across the antennas, but not across time. Under such constraints, it can easily be seen from the above discussion that the average secrecy capacity in fading channels is given by

$$C_s = \frac{1}{n_R} \mathbb{E}_{\mathbf{H}_m, \mathbf{H}_e} \left\{ \max_{\substack{\mathbf{K}_x \succeq \mathbf{0} \\ \text{tr}(\mathbf{K}_x) \leq P}} \log \det \left(\mathbf{I} + \frac{1}{N_m} \mathbf{H}_m \mathbf{K}_x \mathbf{H}_m^\dagger \right) - \log \det \left(\mathbf{I} + \frac{1}{N_e} \mathbf{H}_e \mathbf{K}_x \mathbf{H}_e^\dagger \right) \right\} \quad (37)$$

where the expectation is with respect to the joint distribution of $(\mathbf{H}_m, \mathbf{H}_e)$. Note that the only difference between (4) and (37) is the presence of expectation in (37). Due to this similarity, the following result can be obtained immediately as a corollary to Theorem 1.

Corollary 2: The first derivative of the average secrecy capacity in (37) with respect to SNR at SNR = 0 is

$$\dot{C}_s(0) = \mathbb{E}_{\mathbf{H}_m, \mathbf{H}_e} \{[\lambda_{\max}(\Phi)]^+\} \quad (38)$$

where again $\Phi = \mathbf{H}_m^\dagger \mathbf{H}_m - \frac{N_m}{N_e} \mathbf{H}_e^\dagger \mathbf{H}_e$. The second derivative of the average secrecy capacity at SNR = 0 is given by

$$\ddot{C}_s(0) = -n_R \mathbb{E}_{\mathbf{H}_m, \mathbf{H}_e} \left\{ \min_{\substack{\{\alpha_i\} \\ \alpha_i \in [0,1] \forall i, j=1 \\ \sum_{i=1}^l \alpha_i = 1}} \sum_{j=1}^l \alpha_i \alpha_j \left(|\mathbf{u}_j^\dagger \mathbf{H}_m^\dagger \mathbf{H}_m \mathbf{u}_i|^2 - \frac{N_m^2}{N_e^2} |\mathbf{u}_j^\dagger \mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{u}_i|^2 \right) 1\{\lambda_{\max}(\Phi) > 0\} \right\} \quad (39)$$

where $1\{\cdot\}$ again denotes the indicator function, l is the multiplicity of $\lambda_{\max}(\Phi) > 0$, and $\{\mathbf{u}_i\}$ are the eigenvectors that span the maximum-eigenvalue eigenspace for particular realizations of \mathbf{H}_m and \mathbf{H}_e .

Remark 8: Similarly as in the unfaded case, $\dot{C}_s(0)$ is achieved by always transmitting in the maximum-eigenvalue eigenspace of the realizations of the channel matrices \mathbf{H}_m and \mathbf{H}_e . In order to achieve the second derivative, optimal values of $\{\alpha_i\}$ (or equivalently the optimal power allocation across the antennas) should be identified again for each possible realization of the channel matrices.

Remark 9: In the single-antenna case in which $n_T = n_R = n_E = 1$, the first and second derivatives of the average secrecy capacity become

$$\dot{C}_s(0) = \mathbb{E}_{h_m, h_e} \left\{ \left[|h_m|^2 - \frac{N_m}{N_e} |h_e|^2 \right]^+ \right\} \quad (40)$$

$$\ddot{C}_s(0) = \mathbb{E}_{h_m, h_e} \left\{ \left[|h_m|^4 - \frac{N_m}{N_e} |h_e|^4 \right]^+ \right\}. \quad (41)$$

Corollary 3: The minimum bit energy achieved in fading

channels under secrecy constraints is

$$\frac{E_b}{N_{0, s, \min}} = \frac{\log 2}{\mathbb{E}_{\mathbf{H}_m, \mathbf{H}_e} \{[\lambda_{\max}(\Phi)]^+\}}. \quad (42)$$

Remark 10: Fading has a potential to improve the low-SNR performance and hence the energy efficiency. To illustrate this, we consider the following example. Consider first the unfaded Gaussian channel in which the deterministic channel coefficients are $h_m = h_e = 1$. For this case, we have

$$\dot{C}_s(0) = \left[1 - \frac{N_m}{N_e} \right]^+ \quad \text{and} \quad \frac{E_b}{N_{0, s, \min}} = \frac{\log 2}{\left[1 - \frac{N_m}{N_e} \right]^+}. \quad (43)$$

Now, consider a Rayleigh fading environment and assume that h_m and h_e are independent, zero-mean, Gaussian random variables with variances $E\{|h_m|^2\} = E\{|h_e|^2\} = 1$. Then, we can easily find that

$$\dot{C}_s(0) = \mathbb{E}_{h_m, h_e} \left\{ \left[|h_m|^2 - \frac{N_m}{N_e} |h_e|^2 \right]^+ \right\} = \frac{N_e}{N_m + N_e} \quad (44)$$

leading to $\frac{E_b}{N_{0, s, \min}} = \frac{\log 2}{\frac{N_e}{N_m + N_e}}$. Note that if $N_e > 0$, $\frac{N_e}{N_m + N_e} > \left[1 - \frac{N_m}{N_e} \right]^+$. Hence, fading strictly improves the low-SNR performance by increasing $\dot{C}_s(0)$ and decreasing the minimum bit energy even without performing power control over time. Further gains are possible with power adaptation. Another interesting observation is the following. In unfaded channels, if $N_m \geq N_e$, the minimum bit energy is infinite and secure communication is not possible. On the other hand, in fading channels, the bit energy is finite as long as N_m is finite and $N_e > 0$. Clearly, even if $N_m \geq N_e$, favorable fading conditions enable secure transmission in fading channels.

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355-1367, Oct. 1975
- [2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, pp. 451-456, Jul. 1978.
- [3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 3, pp. 339-348, May 1978.
- [4] Special issue on information-theoretic security, *IEEE Trans. Inform. Theory*, vol. 54, no. 6, June 2008.
- [5] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inform. Theory*, vol. 49, pp. 3235-3249, Dec. 2003.
- [6] Z. Li, W. Trappe, and R. D. Yates, "Secret communication via multi-antenna transmission," 41st Conference on Information Sciences and Systems (CISS), Baltimore, March 2007.
- [7] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 Channel," submitted for publication. Also available at <http://arxiv.org/abs/0709.3541>.
- [8] A. Khisti and G. W. Wornell, "The MIMOME channel," Proc. of the 45th Annual Allerton Conference on Communication, Control, and Computing, October 2007. Also available at <http://arxiv.org/abs/0710.1325>.
- [9] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO Wiretap channel," available at <http://arxiv.org/abs/0710.1920>.
- [10] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wiretap channel," submitted for publication. Also available at <http://arxiv.org/abs/0710.4105>.
- [11] S. Verdú, "Spectral efficiency in the wideband regime," *IEEE Trans. Inform. Theory*, vol. 48, pp. 1319-1343, June 2002.
- [12] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2470 - 2492, June 2008.
- [13] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, 1999.
- [14] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.