Secret-Key Agreement over Spatially Correlated Multiple-Antenna Channels in the Low-SNR Regime

Marwen Zorgui[1], Zouheir Rezki[1], Basel Alomair[2], Eduard A. Jorswieck[3], and Mohamed-Slim Alouini[1]
[1] King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia
[2] The National Center for Cybersecurity Technology (C4C)
King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia
[3] Technische Universität Dresden, Germany
{marwen.zorgui,zouheir.rezki,slim.alouini}@kaust.edu.sa, alomair@kacst.edu.sa, eduard.jorswieck@tu-dresden.de

***Abstract*—We consider secret-key agreement with public discussion over Rayleigh fast-fading channels with transmit, receive and eavesdropper correlation. The legitimate receiver along with the eavesdropper are assumed to have perfect channel knowledge while the transmitter has only knowledge of the correlation matrices. We analyze the secret-key capacity in the low signal-to-noise ratio (SNR) regime. We derive closed-form expressions for the first and the second derivatives of the secret-key capacity with respect to SNR at SNR$= 0$, for arbitrary correlation matrices and number of transmit, receive and eavesdropper antennas. Moreover, we identify optimal transmission strategies achieving these derivatives. For instance, we prove that achieving the first and the second derivatives requires a uniform power distribution between the eigenvectors spanning the maximal-eigenvalue eigenspace of the transmit correlation matrix. We also compare the optimal transmission scheme to a simple uniform power allocation. Finally, we express the minimum energy required for sharing a secret-key bit as well as the wideband slope in terms of the system parameters.**

***Index Terms*—Secret-key agreement, MIMO systems, correlation, beamforming, low-SNR regime, energy efficiency.**

I. Introduction

Energy efficiency is of paramount importance in modern wireless communication systems. It has driven a lot of research aiming at better understanding the energy performance limits of wireless communication systems. The low signal-to-noise ratio (SNR) regime turns out to be of particular interest for this kind of analysis. Indeed, it is well-known that for many channel models, energy efficiency improves as one operates at lower signal-to-noise ratio (SNR) regime, and moreover, the minimum energy per bit is achieved as SNR vanishes asymptotically to zero [1]. It is interesting to analyze the impact additional requirement of confidentiality induces on the energy efficiency of wireless communications with secrecy constraint. In [2], the author considers the secrecy capacity of a multiple-input multiple-output (MIMO) wiretap channel in the low-SNR regime. In [3], considering a quasi-static fading setting, the secret-key capacity is studied in the low-power regime. In the fast-fading scenario, correlation impacts the capacity of the system. Correlation emerges in many practical scenarios in wireless communication, e.g., in the absence of enough local scatterers or due to insufficient antenna spacing. In this paper, we consider a fast-fading setting and we aim at studying the impact of correlation on the secret-key capacity in the low-power regime and characterize the energy efficiency behavior of the system under such assumptions.

The work of Z. Rezki and M. -S. Alouini was supported by the Qatar National Research Fund (a member of Qatar Foundation) under NPRP Grant NPRP 5-603-2-243. The statements made herein are solely the responsibility of the authors. This work has been supported by King Abdulaziz City of Science and Technology (KACST), Riyadh, Saudi Arabia. The work of E. Jorswieck is partly supported by the German Research Foundation (DFG) within the Cluster of Excellence "Center for Advancing Electronics Dresden (cfaed)".

II. System model and preliminaries

We consider the problem of secret-key agreement between a legitimate transmitter and a legitimate receiver in the presence of an eavesdropper who overhears transmissions broadcasted over the wireless medium [4]. The transmitter, destination and eavesdropper are equipped with m_S, m_D and m_E antennas, respectively. For each channel use, the channel is represented as follows

$$\begin{aligned}\mathbf{y}_D(i) &= \mathbf{H}_D(i)\mathbf{x}(i) + \mathbf{n}_D(i)\\ \mathbf{y}_E(i) &= \mathbf{H}_E(i)\mathbf{x}(i) + \mathbf{n}_E(i),\end{aligned} \tag{1}$$

where index $i, i = 1, \ldots, n$, designates time instant i, and

- $\mathbf{x}(i)$ is the $m_S \times 1$ complex-valued transmitted symbol vector,
- $\mathbf{y}_D(i)$ (resp. $\mathbf{y}_E(i)$) is the $m_D \times 1$ (resp. $m_E \times 1$) complex-valued received symbol vector at the destination (resp. at the eavesdropper),
- $\mathbf{n}_D(i)$ (resp. $\mathbf{n}_E(i)$) is the $m_D \times 1$ (resp. $m_E \times 1$) noise vector with i.i.d. circular-symmetric complex Gaussian entries $\sim \mathcal{CN}(0, \sigma_D^2)$ (resp. $\sim \mathcal{CN}(0, \sigma_E^2)$),
- $\mathbf{H}_D(i)$ (resp. $\mathbf{H}_E(i)$) is the $m_D \times m_S$ (resp. $m_E \times m_S$) channel matrix from the source to the destination (resp. the eavesdropper).

The transmitter is constrained in its total power. We denote the input covariance matrix by $\mathbf{Q} = \mathbb{E}[\mathbf{x}\mathbf{x}^\dagger]$. Then, we have

$$\mathrm{Tr}(\mathbf{Q}) \leq P. \tag{2}$$

The signal-to-noise ration is defined as SNR $= \frac{P}{\sigma_D^2}$. The effect of correlation is captured using the Kronecker model as in [5]:

$$\begin{aligned}\mathbf{H}_D &= \mathbf{R}_D^{1/2}\mathbf{W}_D\mathbf{R}_T^{1/2}\\ \mathbf{H}_E &= \mathbf{R}_E^{1/2}\mathbf{W}_E\mathbf{R}_T^{1/2},\end{aligned} \tag{3}$$

where $\mathbf{W}_D$ (resp. $\mathbf{W}_E$) is $m_D \times m_S$ (resp. $m_E \times m_S$) matrix with i.i.d entries $\sim \mathcal{CN}(0,1)$. $\mathbf{R}_T$, $\mathbf{R}_D$ and $\mathbf{R}_E$ correspond to the transmit correlation matrix, the destination correlation matrix and the eavesdropper correlation matrix, respectively. The destination and the eavesdropper have perfect knowledge

about their incoming channels while the transmitter has only knowledge about correlation matrices. In [5], it is shown that the secret-key capacity can be expressed as

$$C = \max_{\mathrm{Tr}(\mathbf{Q})\leq P} \mathbb{E}\left[\log \frac{\left|\mathbf{I}_{m_D+m_E} + \mathbf{H}\mathbf{Q}\mathbf{H}^\dagger\right|}{\left|\mathbf{I}_{m_E} + \frac{1}{\sigma_E^2}\mathbf{H}_E\mathbf{Q}\mathbf{H}_E^\dagger\right|}\right], \ \mathbf{H} = \begin{bmatrix}\frac{1}{\sigma_D}\mathbf{H}_D \\ \frac{1}{\sigma_E}\mathbf{H}_E\end{bmatrix}. \quad (4)$$

III. Low-SNR regime

In the sequel, we express the secret-key capacity and its derivatives as a function of SNR.

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

Theorem 1. The first derivative of the secret-key capacity in (4) with respect to SNR at SNR$= 0$ is

$$\dot{C}(0) = m_D\lambda_1^T, \quad (6)$$

where λ_1^T denotes the maximal eigenvalue of $\mathbf{R}_T$. Moreover, $\dot{C}(0)$ can be achieved by choosing the input covariance matrix of the form

$$\mathbf{Q} = P\sum_{i=1}^{L}\alpha_i\mathbf{u}_i\mathbf{u}_i^\dagger, \quad (7)$$

where $\mathbf{u}_i$ are the eigenvectors that span the maximal-eigenvalue eigenspace of $\mathbf{R}_T$, α_i are non-negative coefficients that sum to unity and L denotes the multiplicity of λ_1^T.

Thus, transmitting in the maximal-eigenvalue eigenspace is necessary to achieve $\dot{C}(0)$, regardless of how power is distributed between the eigenvectors associated with λ_1^T.

Remark 1. Theorem 1 shows that transmit correlation helps increase the secret-key capacity in the low-SNR regime. For instance, the larger transmit correlation (larger is to be understood in the majorization sense of [6]), the higher the value of λ_1^T and therefore the higher the secret-key capacity.

We now consider the second derivative. For that, we assume that the input covariance matrix is chosen as in (7) and our result is summarized in Theorem 2.

Theorem 2. The second derivative of the secret-key capacity in (4) with respect to SNR at SNR$= 0$ is

$$\ddot{C}(0) = -\frac{{\lambda_1^T}^2}{L}\left[L\mathrm{Tr}\left(\mathbf{R}_D^2\right) + 2\frac{\sigma_D^2}{\sigma_E^2}m_Dm_E + m_D^2\right]. \quad (8)$$

Moreover, to achieve $\ddot{C}(0)$, it is necessary to distribute power equally in each orthogonal direction in the maximal-eigenvalue eigenspace of $\mathbf{R}_T$, i.e., $\mathbf{Q} = \frac{P}{L}\sum_{i=1}^{L}\mathbf{u}_i\mathbf{u}_i^\dagger$.

If λ_1^T has multiplicity one, $\ddot{C}(0)$ is achieved with $\mathbf{Q} = P\mathbf{u}_1\mathbf{u}_1^\dagger$ where $\mathbf{u}_1$ is the eigenvector that corresponds to λ_1^T. Thus, beamforming in the direction in which $\mathbf{R}_T$ is maximized is optimal in the sense of achieving the first and the second derivatives of the secret-key capacity in the low-SNR regime.

A. Non optimal strategy

We study the low-SNR performance when the transmitter allocates power uniformly, i.e., $\mathbf{Q} = \frac{1}{m_S}\mathbf{I}$. We summarize the results in the following proposition.

Proposition 1. The first and the second derivatives achieved by a uniform power allocation strategy are given by

$$\dot{\mathcal{I}}_{unif}(0) = m_D \quad (9)$$

$$\ddot{\mathcal{I}}_{unif}(0) = -\frac{1}{m_S^2}\left[\mathrm{Tr}(\mathbf{R}_T^2)(m_D^2 + 2{\frac{\sigma_D}{\sigma_E}}^2 m_Dm_E) + m_S^2\mathrm{Tr}(\mathbf{R}_D^2)\right], \quad (10)$$

Clearly, $\dot{\mathcal{I}}_{unif}(0) \leq \dot{C}(0)$ which explains the inefficiency of uniform power allocation in the low-power regime. Nonetheless, as simulations suggest, the performance of a uniform power allocation is comparable to the optimal strategy in the low-SNR regime, which can be explained by observing that $\ddot{\mathcal{I}}_{unif}(0) - \ddot{C}(0) \geq 0$.

IV. Minimum Energy per Secret-key bit

The first and the second derivatives of the secret-key capacity at vanishing SNR are closely related to the energy performance measures, namely the minimum energy required for sharing a secret-key bit and the wideband slope. We start by stating the following lemma.

Lemma 1. The secret-key capacity achieved under the average power constraint $\mathbb{E}\|\mathbf{x}\|^2 \leq P$ is a concave function of SNR.

The energy per secret-key bit normalized by the noise variance at the legitimate receiver is defined as

$$\frac{E_b}{N_0}_{sk} = \frac{\mathrm{SNR}}{C(\mathrm{SNR})}\log 2. \quad (11)$$

By virtue of Lemma 1, the secret-key capacity is a concave function of SNR. Therefore, the minimum energy per secret-key bit is achieved in the limit of low-SNR; i.e., SNR $\to 0$. Thus, the minimum energy per secret-key bit and the wideband slope (in bits/s/Hz/(3 dB)) are given by [1, Theorem 5]

$$\frac{E_b}{N_0}_{sk,min} = \frac{\log 2}{\dot{C}(0)}, \ \mathcal{S}_0 = \frac{2\left[\dot{C}(0)\right]^2}{-\ddot{C}(0)}. \quad (12)$$

Using the expressions of (6) and (8), we obtain:

$$\frac{E_b}{N_0}_{sk,min} = \frac{\log 2}{m_D\lambda_1^T}. \quad (13)$$

$$\mathcal{S}_0 = \frac{2m_D^2L}{L\mathrm{Tr}\left(\mathbf{R}_D^2\right) + 2\frac{\sigma_D^2}{\sigma_E^2}m_Dm_E + m_D^2}. \quad (14)$$

References

[1] S. Verdu, "Spectral efficiency in the wideband regime," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1319–1343, Jun 2002.

[2] M. Gursoy, "Secure Communication in the Low-SNR Regime," *IEEE Trans. Commun*, vol. 60, no. 4, pp. 1114–1123, April 2012.

[3] F. Renna, M. Bloch, and N. Laurenti, "Semi-blind key-agreement over MIMO fading channels," *IEEE Trans. Commun*, vol. 61, no. 2, pp. 620–627, February 2013.

[4] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography–part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, 1993.

[5] M. Zorgui, Z. Rezki, B. Alomair, and M.-S. Alouini, "Secret-key agreement over spatially correlated fast-fading multiple-antenna channels with public discussion," in *IEEE International Symposium on Information Theory Proceedings (ISIT'2015), Hong Kong*, Juin 2015.

[6] E. Jorswieck and H. Boche, "Optimal transmission strategies and impact of correlation in multiantenna systems with different types of channel state information," *IEEE Trans. Signal Process*, vol. 52, no. 12, pp. 3440–3453, Dec 2004.