This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

Secure Multiple-Antenna Block-Fading Wiretap Channels with Limited CSI Feedback

Amal Hyadi, *Student Member, IEEE*, Zouheir Rezki, *Senior Member, IEEE*, and Mohamed-Slim Alouini, *Fellow, IEEE*

***Abstract*—In this paper, we investigate the ergodic secrecy capacity of a block-fading wiretap channel with limited channel knowledge at the transmitter. We consider that the legitimate receiver, the eavesdropper and the transmitter are equipped with multiple antennas and that the receiving nodes are aware of their respective channel matrices. The transmitter, on the other hand, is only provided by a B-bit feedback of the main channel state information. The feedback bits are sent by the legitimate receiver, at the beginning of each fading block, over an error-free public link with limited capacity. The statistics of the main and the eavesdropper channel state information are known at all nodes. Assuming an average transmit power constraint, we establish upper and lower bounds on the ergodic secrecy capacity. Then, we present a framework to design the optimal codebooks for feedback and transmission. In addition, we show that the proposed lower and upper bounds coincide asymptotically as the capacity of the feedback link becomes large, i.e. $B \to \infty$; hence, fully characterizing the ergodic secrecy capacity in this case. Besides, we analyze the asymptotic behavior of the presented secrecy rates, at high Signal-to-Noise Ratio (SNR), and evaluate the gap between the bounds.**

***Index Terms*—Ergodic secrecy capacity, channel state information, multiple-antenna, block-fading channel, limited feedback, high SNR.**

I. Introduction

The broadcast nature of the wireless channel makes radio transmissions vulnerable to eavesdropping attacks. To date, the security of wireless communications is mainly performed at the application layer using cryptographic techniques. However, with the emergence of ad-hoc and decentralized networks, these high-level techniques turn out to be complex and challenging to implement. Therefore, there has been a significant recent interest in studying the inherent ability of the physical layer to provide secure communications. This paradigm is known as Wireless Physical Layer Security.

The research reported in this publication was supported by CRG 2 grant from the Office of Sponsored Research at King Abdullah University of Science and Technology (KAUST). This work was presented in part at the 2015 IEEE Global Communications Conference (GLOBECOM'2015), San Diego, CA, USA. The statements made herein are solely the responsibility of the authors.

A. Hyadi and M.-S. Alouini are with the Division of Computer, Electrical, and Mathematical Sciences & Engineering (CEMSE), King Abdullah University of Science and Technology (KAUST), Thuwal, Makkah Province, Saudi Arabia. [e-mail: {amal.hyadi, slim.alouini}@kaust.edu.sa].

Z. Rezki is with the Electrical and Computer Engineering Department, University of Idaho, Moscow, ID, US. [e-mail: zrezki@uidaho.edu].

A. Literature Review

The first significant results in the area of physical layer security were presented in [1] and [2]. In [1], Wyner introduced the degraded wiretap channel where a source communicates with one receiver over a discrete, memoryless channel in the presence of an eavesdropper observing the legitimate channel's output. Wyner proved that, for such a system, there exists a coding scheme that ensures the reliability of the communication while asymptotically leaking no information to the eavesdropper. In [2], Csiszár and Körner reconsidered Wyner's wiretap channel for the case of a non-degraded communication, i.e., the main and the eavesdropper's channels are supposed to be independent of each other. Ulterior works generalized Wyner's, and Csiszár and Körner's works to the case of Gaussian channels [3] and fading channels [4], [5].

Multiple-input multiple-output (MIMO) systems have an increasingly important part to play in emerging wireless communication networks. In fact, when used with appropriately designed signal processing algorithms, multiple antenna arrays can considerably enhance the network performance [6], [7]. The problem of analyzing the secrecy capacity of multiple antenna systems has been of great interest in last years. In [8], the authors investigated the secrecy capacity of the multiple-input single-output (MISO) wiretap Gaussian channel and presented an upper bound on the secrecy capacity for the MIMO case with an asymptotic signal to noise ratio (SNR). Another work [9] characterized the secrecy capacity for the MISO case, with a multiple-antenna eavesdropper, when the main and the eavesdropping channels are known to all terminals. The secrecy capacity of the MISO wiretap Gaussian channel was also investigated in [10] and [11]. The secrecy capacity of MIMO Gaussian channels with a single antenna eavesdropper was examined in [12], and the case of MIMO transmission with a multiple-antenna eavesdropper has been considered in [13]–[16] when the channel matrices are fixed and known to all terminals.

Transmit beamforming is one of the typical approaches to achieve full diversity in MIMO wireless systems. Unfortunately, to obtain the optimal performance, this method requires a full knowledge of the channel state information (CSI) at the transmitter (CSIT), or the knowledge of the optimal beamforming vector. However, this complete knowledge is difficult to have in practical scenarios as the acquisition of the CSIT requires the receiver to feedback its CSI constantly to the transmitter. This feedback process is usually accompanied by the introduction of uncertainty into the CSIT. Different

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

phenomena can cause the CSIT to be imperfect. Most commonly, the uncertainty comes from an error of estimation at the transmitter, from a feedback link with finite capacity, or from a delayed feedback. Studying the impact of channel uncertainty on physical layer security has been the focus of a number of research works, in the last few years. Among these works, [17]–[21] examined the case when the uncertainty is the result of an error of estimation, and [22]–[24] analyzed the wiretap channel with outdated CSI. A synopsis of how different levels of CSIT impact the system's security is provided in [25] and a detailed state-of-the-art review of physical layer security with CSIT uncertainty is presented in [26].

In this paper, we consider the case when the channel uncertainty is the result of limited CSI feedback, and we examine the impact of this uncertainty on the ergodic secrecy capacity of multiple antenna block-fading wiretap channels. With no secrecy constraints, the finite feedback problem has been extensively studied in the literature [27]–[33]. The secrecy throughput when the feedback is finite has been investigated in [34] for single antenna wiretap channels, in [35] and [36] for MIMO block-fading channels, and in [37] for the fast fading MIMO case. The noise leakage problem when transmitting artificial noise (AN) with limited CSI feedback was analyzed in [38] and [39]. The authors in [38] consider the case when the transmitter is equipped with multiple antennas while the legitimate receiver and the eavesdropper have only one antenna. The aim of the work is to maximize the throughput under a connection outage constraint and a secrecy outage constraint. Concerning the impact of having finite feedback, the authors show that it is more important to feedback the channel direction information (CDI) to reduce the noise leakage problem. The paper also points out that with only limited feedback from the desired receiver, the secrecy throughput remains bounded even with an arbitrarily large transmit power. Similar conclusions were drawn in [39], where the noise leakage problem was analyzed for multiple antenna systems with the number of antennas at the transmitter being larger than the total number of antennas at the legitimate receiver and the eavesdropper. Analysis on the use of artificial noise to enhance the equivocation rate are presented in, e.g., [40]–[42].

B. Contributions Summary

In this work, we investigate the ergodic secrecy capacity of multiple-antenna block-fading wiretap channels with limited CSI feedback. Likewise [4] and [34], we assume that the coherence blocks are large enough so that reliable communication is feasible over each block. Furthermore, we consider that the transmitter is unaware of the channel matrices of neither the main nor the eavesdropper channels, and is only provided by a finite CSI feedback sent by the legitimate receiver through a public, error-free, link with limited capacity. Assuming an average power constraint at the transmitter, we provide two achievable secrecy rates and an upper bound on the ergodic secrecy capacity. The first secrecy rate is achieved by using the feedback information not only to adapt the power but also to adjust the transmission rate during each fading block. The considered scheme guarantees that the best the eavesdropper can receive, during a given fading block, is the fixed transmission rate received at the legitimate node. For the second achievable secrecy rate, the feedback is mainly employed for the power adaptation purpose. Besides, in order to maximize the secrecy rate, we present a framework to design the used codebboks for feedback and transmission. The presented framework is based on the iterative Lloyd's algorithm [43]. For the particular case of infinite feedback, we prove that the first achievable secrecy rate and the presented upper bound on the ergodic secrecy capacity coincide, hence, fully characterizing the ergodic secrecy capacity in this case. The high-SNR regime and the secrecy degrees of freedom (SDoF) of the system are also investigated in this work. It is worth mentioning that we do not consider the transmission of AN in the proposed achievable secrecy rates. However, we do compare our results to the ones in, e.g., [39], through simulations. In particular, the main differences between [39] and our work can be summarized as follows

- The work in [39] investigates the impact of having limited CSI feedback on the secrecy rate achieved by AN transmission. Since AN needs to be imposed in the null space of the legitimate receiver's channel in order to disrupt the eavesdropper's reception, the authors consider the case when the number of transmit antennas is larger than the total number of antennas at both the legitimate receiver and the eavesdropper, i.e., $N_{\mathrm{T}} \geq N_{\mathrm{R}} + N_{\mathrm{E}}$. Otherwise, the achievable secrecy rate is equal to zero. In this work, we examine the problem under no assumptions on the number of antennas deployed at the communicating nodes, and through our simulations, we can see that the proposed achievable secrecy rates can still achieve a non-zero secrecy rate even when $N_{\mathrm{T}} < N_{\mathrm{R}} + N_{\mathrm{E}}$.
- Since [39] studies the impact of finite feedback on AN transmission, the feedback bits are used to inform the transmitter about the CDI. The authors adopt the random quantization codebook model proposed and studied by [44] to evaluate the problem. In this work, we present an offline hybrid beamforming and adaptive power-control framework to design the quantization codebooks. The framework is formulated in such a way to maximize the achievable secrecy rate.
- When the number of feedback bits B is fixed, the achievable secrecy rate, presented in [39], is upper bounded by a constant regardless of the transmission power. This is not the case when the transmitter has perfect CDI. Therefore, to maintain a constant secrecy rate loss (compared to the perfect CDI case), the authors in [39] show that B must scale logarithmically with the average transmission power. In this work, the proposed achievable secrecy rates can still scale with the average transmission power even when B is fixed. This could be seen from the presented asymptotic analysis and simulations.

C. Outline of the Paper

The paper is organized as follows. Section II describes the system model. The main results are summarized in Section III; the ergodic secrecy capacity is characterized in subsection III-A, an asymptotic analysis in the high SNR regime

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

is presented in subsection III-B, and an optimal framework for feedback and transmission is provided in subsection III-C. In Section IV, we present details on the characterization of the achievable ergodic secrecy rates and the upper bound on the ergodic secrecy capacity. Finally, selected simulation results are illustrated in Section V, and Section VI concludes the paper.

Notations: Throughout the paper, we use the following notational conventions. The expectation operation is denoted by $\mathbb{E}[.]$, the conditional expectation, given event A, is represented by $\underset{.|A}{\mathbb{E}}[.]$, log denotes the natural logarithm unless otherwise indicated, and we define $\{\nu\}^+ = \max(0, \nu)$. The entropy of a discrete random variable $\mathbf{X}$ is denoted by $H(\mathbf{X})$, and the mutual information between random variables $\mathbf{X}$ and $\mathbf{Y}$ is denoted by $I(\mathbf{X};\mathbf{Y})$. We also use the notation $\mathbf{X}\sim\mathcal{CN}(\mu, \mathbf{\Sigma})$ to indicate that $\mathbf{X}$ is a circularly symmetric complex-valued Gaussian random vector with mean vector μ and covariance matrix $\mathbf{\Sigma}$. A sequence of length n is denoted by $\mathbf{X}^n$, $\mathbf{X}(k)$ represents the k-th element of $\mathbf{X}^n$, and $\mathbf{X}(l,k)$ the k-th element of $\mathbf{X}^n$ in the l-th fading block. In addition, we use $||.||$ for the Euclidean norm, the superscript * for the Hermitian transpose of a matrix, and the symbols tr[.] and $|.|$ for the trace and the determinant, respectively. The notation $\mathbf{X} \succeq 0$ indicates that $\mathbf{X}$ is positive semidefinite, and we use $\mathbf{I}_N$ to denote the identity matrix of size N.

II. System Model

We consider a discrete-time memoryless wiretap channel where a transmitter wants to communicate a secret message to a legitimate receiver in the presence of an eavesdropper. The model of interest consists of a multiple-antenna channel with N_{T} transmit antennas, N_{R} receive antennas at the legitimate receiver, and N_{E} receive antennas at the eavesdropper. The respective received signals at the intended receiver and the eavesdropper, at time instant t, are given by

$$\begin{aligned} \mathbf{Y}_{\mathrm{R}}(t) &= \mathbf{H}_{\mathrm{R}}(t)\mathbf{X}(t) + \mathbf{Z}_{\mathrm{R}}(t) \\ \mathbf{Y}_{\mathrm{E}}(t) &= \mathbf{H}_{\mathrm{E}}(t)\mathbf{X}(t) + \mathbf{Z}_{\mathrm{E}}(t) \end{aligned} \tag{1}$$

where $\mathbf{X}(t)$ is the transmitted signal, $\mathbf{H}_{\mathrm{R}}(t) \in \mathbb{C}^{N_{\mathrm{R}}\times N_{\mathrm{T}}}$ and $\mathbf{H}_{\mathrm{E}}(t) \in \mathbb{C}^{N_{\mathrm{E}}\times N_{\mathrm{T}}}$ are the complex channel gain matrices, and $\mathbf{Z}_{\mathrm{R}}(t)\sim\mathcal{CN}(0, \sigma_{\mathrm{R}}^2\mathbf{I}_{N_{\mathrm{R}}})$ and $\mathbf{Z}_{\mathrm{E}}(t)\sim\mathcal{CN}(0, \sigma_{\mathrm{E}}^2\mathbf{I}_{N_{\mathrm{E}}})$ are independent and identically distributed (i.i.d.) additive complex Gaussian noise vectors. We consider a block-fading channel where the channel gain matrices remain constant within a fading block of length $\kappa>>1$, i.e., $\mathbf{H}_{\mathrm{R}}(\kappa l) = \mathbf{H}_{\mathrm{R}}(\kappa l - 1) = \cdots = \mathbf{H}_{\mathrm{R}}(\kappa l - \kappa + 1)$ and $\mathbf{H}_{\mathrm{E}}(\kappa l) = \mathbf{H}_{\mathrm{E}}(\kappa l - 1) = \cdots = \mathbf{H}_{\mathrm{E}}(\kappa l - \kappa + 1)$, where $l = 1, \cdots, L$, and L is the total number of fading blocks. In the rest of this paper, we denote the respective main and eavesdropper channel gain matrices, during the l th fading block, as $\mathbf{H}_{\mathrm{R}}(l)$ and $\mathbf{H}_{\mathrm{E}}(l)$, $l = 1, \cdots, L$. We assume that the channel encoding and decoding frames span a large number of fading blocks, i.e., L is large, that the blocks change independently from a fading block to another, and that the entries of $\mathbf{H}_{\mathrm{R}}$ and $\mathbf{H}_{\mathrm{E}}$ have bounded distributions. The channel input $\{\mathbf{X}(t)\}_t$ is subject to an average total power constraint

$$\frac{1}{n}\sum_{t=1}^{n} ||\mathbf{X}(t)||^2 \leq P_{\text{avg}}, \tag{2}$$

where $n=\kappa L$. We assume perfect CSI at the receiver sides. That is, the legitimate receiver is instantaneously aware of its channel gain matrix $\mathbf{H}_{\mathrm{R}}(l)$, and the eavesdropper knows $\mathbf{H}_{\mathrm{E}}(l)$, with $l = 1, \cdots, L$. The statistics of the main and the eavesdropping channels are available to all nodes. Further, we assume that the transmitter is not aware of the instantaneous channel realizations of neither channel. However, the legitimate receiver provides the transmitter with a B-bit CSI feedback through an error-free channel with limited capacity. This feedback is transmitted at the beginning of each fading block and is also tracked by the eavesdropper. A block diagram of the communication system is presented in Fig. 1, where ENC represents the encoder at the transmitter, B&PC is the beamforming and power control entity, and $\mathrm{DEC_R}$ and $\mathrm{DEC_E}$ are the respective decoders at the legitimate receiver and the eavesdropper.

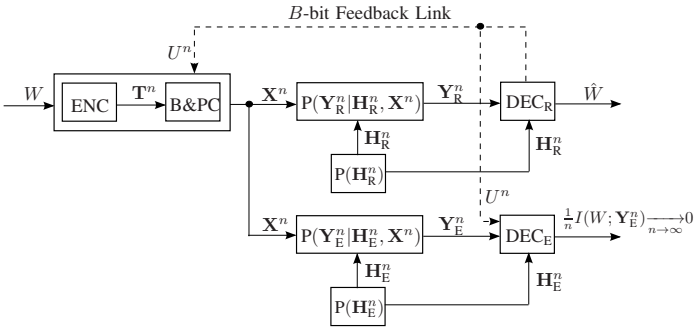

Fig. 1. Block diagram of the channel model.

The transmitter wishes to send a secret message W to the legitimate receiver. A $(2^{n\mathcal{R}_{\mathrm{s}}}, n)$ code consists of the following elements:

- A message set $\mathcal{W} = \left\{1, 2, \cdots, 2^{n\mathcal{R}_{\mathrm{s}}}\right\}$ with the messages $W \in \mathcal{W}$ independent and uniformly distributed over $\mathcal{W}$;
- A stochastic encoder $f : \mathcal{W} \to \mathcal{X}^n$ that maps each message w to a codeword $\mathbf{X}^n \in \mathcal{X}^n$;
- A decoder at the legitimate receiver $g : \mathcal{Y}^n \to \mathcal{W}$ that maps a received sequence $\mathbf{Y}_{\mathrm{R}}^n \in \mathcal{Y}^n$ to a message $\hat{w} \in \mathcal{W}$.

A rate $\mathcal{R}_{\mathrm{s}}$ is an *achievable secrecy rate* if there exists a sequence of $(2^{n\mathcal{R}_{\mathrm{s}}}, n)$ code such that both the average error probability, $P_{\mathrm{e}} = \frac{1}{2^{n\mathcal{R}_{\mathrm{s}}}}\sum_{w=1}^{2^{n\mathcal{R}_{\mathrm{s}}}} \Pr\left[W \neq \hat{W}\middle|W = w\right]$, and the leakage rate at the eavesdropper, $\frac{1}{n}I(W;\mathbf{Y}_E^n, \mathbf{H}_E^n, \mathbf{H}_R^n, U^n)$, go to zero as n goes to infinity. The *secrecy capacity* $\mathcal{C}_{\mathrm{s}}$ is defined as the maximum achievable secrecy rate, i.e., $\mathcal{C}_{\mathrm{s}} \triangleq \sup \mathcal{R}_{\mathrm{s}}$, where the supremum is over all achievable secrecy rates.

Note that, we give the eavesdropper all channels to strengthen the secrecy results. This could be seen as a worst case scenario where the eavesdropper is not only aware of its channel matrix $\mathbf{H}_{\mathrm{E}}$, and the B-bit CSI feedback transmitted

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

by the legitimate receiver, but it also knows the legitimate receiver's channel matrix $\mathbf{H}_{\mathrm{R}}$. It is, however, important to note that the knowledge of matrix $\mathbf{H}_{\mathrm{R}}$ will not be advantageous for the eavesdropper since given the received signal at the eavesdropper $\mathbf{Y}_{\mathrm{E}}$, the channel matrix $\mathbf{H}_{\mathrm{E}}$, and the feedback information U, the transmitted signal $\mathbf{X}$, is independent of the main channel matrix $\mathbf{H}_{\mathrm{R}}$, i.e., $H(\mathbf{X}|\mathbf{Y}_{\mathrm{E}}^n, \mathbf{H}_{\mathrm{E}}^L, \mathbf{H}_{\mathrm{R}}^L, U^L) = H(\mathbf{X}|\mathbf{Y}_{\mathrm{E}}^n, \mathbf{H}_{\mathrm{E}}^L, U^L)$.

A. Feedback Channel Model

For every fading block, and prior to payload data transmission, a preamble signal is sent to the legitimate receiver in order to estimate its channel gain. This preamble transmission is also tracked by the eavesdropper who gets to estimate its channel too. We assume that the channel gain matrices are perfectly estimated at the receiving sides. This is achievable for asymptotically large fading blocks [45]. Also, we consider that the feedback channel capacity is constrained to B bits per fading block, i.e., $\log_2|\mathcal{U}| \leq B$, with $|\mathcal{U}|$ denoting the cardinality of the set, $\mathcal{U}$, of feedbacked symbols.

In the light of the work in [32], the adopted feedback strategy consists on partitioning the space of the main channel gain into Q regions $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$, where $Q = 2^B$. Knowing $\mathbf{H}_{\mathrm{R}}$ perfectly, the legitimate receiver determines in which region, $\mathcal{H}_q$ with $q{=}1, \cdots, Q$, the channel matrix lies. Also, the legitimate receiver associates the partition index q with each region $\mathcal{H}_q$, and transmits the index codeword u_q through the feedback channel.

B. Adaptive Beamforming and Power Control Model

At the transmitter side, in addition to an encoder for secrecy, the confidential forward transmission is adapted using beamforming and power control. Since the only information available to the transmitter, about the main channel gain, is obtained through the limited feedback link, the choice of the relevant transmission strategy is based on what was feedbacked. In fact, each feedbacked information u_q corresponds to a Hermitian beamforming matrix $\mathbf{V}_q$ and a diagonal power control matrix $\mathbf{\Lambda}_q$ with $q = 1, \cdots, Q$. That is, for each fading block, the transmitter uses the feedbacked information to apply the appropriate beamforming matrix and power control matrix to the encoded symbol $\mathbf{T}$. The forward signal $\mathbf{X}$ can then be written in the form $\mathbf{X} = \mathbf{V}_q \mathbf{\Lambda}_q^{1/2} \mathbf{T}$, and we let $\mathbb{E}[\mathbf{T}\mathbf{T}^*]{=}\mathbf{I}_{N_{\mathrm{T}}}$ for normalization. By taking $\boldsymbol{\rho}_q{=}\mathbf{V}_q\mathbf{\Lambda}_q\mathbf{V}_q^*$, the respective received SNRs at the legitimate receiver and the eavesdropper are $\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*$ and $\frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{E}}^*$.

The adopted feedback and transmission strategies require the construction of a codebook for the partitioning of the main channel gain space into Q regions, as well as a codebook for the associated set of beamforming and power control matrices. In this work, we propose a design of fixed feedback and transmission codebooks that optimizes the secrecy performance of the system. Indeed, we present a framework to find the optimal feedback strategy $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$, as well as the optimal transmission strategy $\{\boldsymbol{\rho}_1, \cdots, \boldsymbol{\rho}_Q\}$, such that the average power constraint is satisfied, i.e., $\mathrm{tr}\left[\mathbb{E}[\boldsymbol{\rho}_q]\right] \leq P_{\mathrm{avg}}$, matrix $\boldsymbol{\rho}_q$ is positive semi-definite, i.e., $\boldsymbol{\rho}_q \succeq 0$, and the secrecy rate is maximized. It is assumed that all nodes are aware of the codebooks used for feedback and transmission. More details on the codebooks generation are available in the following section.

III. Main Results

In this section, we start by characterizing the ergodic secrecy capacity of the considered multiple-antenna system. Then, to better understand the correlation between the obtained expressions and the system's parameters, we present an asymptotic analysis of the results. The SDoF of the system is also analyzed. Finally, a framework characterizing the generation of optimal codebooks for the feedback and the transmission strategies is introduced.

A. Lower and Upper Bounds on the Ergodic Secrecy Capacity

Theorem 1: For the discrete-time memoryless multiple-antenna wiretap channel described in (1), with an error-free B-bit CSI feedback link, sent at the beginning of each fading block, and the average power constraint in (2), the following secrecy rates are achievable

$$\mathcal{C}_{\mathrm{s}}^{-} = \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q, \boldsymbol{\rho}_q\}} \mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\left\{ \log \frac{\min\limits_{\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{E}}^*\right|} \right\}^{+} \right] P_q, \tag{3}$$

$$\widetilde{\mathcal{C}}_{\mathrm{s}}^{-} = \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q, \boldsymbol{\rho}_q\}} \mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}}, \mathbf{H}_{\mathrm{R}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\log \frac{\left|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{E}}^*\right|} \right] P_q, \tag{4}$$

where $Q{=}2^B$, $\mathrm{tr}\left[\mathbb{E}[\boldsymbol{\rho}_q]\right] {\leq} P_{\mathrm{avg}}$, $\boldsymbol{\rho}_q {\succeq} 0$, and $P_q{=}\Pr\left[\mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q\right]$ for all $q \in \{1, \cdots, Q\}$.

Proof: A detailed proof of Theorem 1 is provided in the following section. Here, we outline the achievability schemes.

- *Achievability scheme for $\mathcal{C}_{\mathrm{s}}^{-}$*: We adopt a variable rate transmission controlled by the feedback information sent by the legitimate receiver. Thereby, during each fading block, if the main channel gain matrix falls within the partition region $\mathcal{H}_q$, the transmitter conveys codewords at rate $R_q = \min\limits_{\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \log\left|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|$, with the transmission strategy $\boldsymbol{\rho_q}$. Rate R_q changes only periodically and is held constant over the duration interval of a fading block. Let $\mathbf{T}_q$ be a channel gain matrix from $\mathcal{H}_q$ satisfying $\mathbf{T}_q = \arg\min\limits_{\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|$. The considered scheme guarantees that when the channel to the eavesdropper is better than the worst main channel gain in region $\mathcal{H}_q$, the mutual information between the transmitter and the eavesdropper is upper bounded by R_q. Otherwise, this mutual information will be $\log\left|\mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{E}}^*\right|$. We can then optimize over the main channel gain regions, $\mathcal{H}_q$'s, and the transmission strategies, $\boldsymbol{\rho}_q$'s, to maximize the secrecy rate.
- *Achievability scheme for $\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}$*: The proposed feedback and transmission procedure can be seen as a deterministic mapping that associates each feedback information

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

with an appropriate transmission strategy. Accordingly, the adopted communication system can be equivalently modeled as a multiple-antenna memoryless channel without feedback where the mapping function becomes an amplification component of the new channel.

Intuitively, Theorem 1 states that even a 1-bit CSI feedback, sent at the beginning of each fading block, ensures a positive secrecy rate. of course, the more the transmitter knows the better the secrecy performances are. As a matter of fact, increasing the number of feedback bits B, also increases the mutual information between the transmitted feedback information and the actual channel gain matrix. More specifically, when B increases, equivalently Q increases, the partitions $\{\mathcal{H}_q\}_q^Q$ will provide a better characterization for matrix $\mathbf{H}_{\mathrm{R}}$. That is, the transmitter will end up with more information about the main channel gain, which will allow a better adaptation of the transmission strategy and, hence, the achievement of a higher secrecy rate. It is also worth mentioning that the main difference between the two achieving schemes is that, in the first scheme, we use the feedback information to adapt both the transmission rate and the power, whereas in the second scheme, the feedback is only used to adapt the power.

We now present an upper bound on the ergodic secrecy capacity with limited CSI feedback.

Theorem 2: For the discrete-time memoryless multiple-antenna wiretap channel described in (1), with an error-free B-bit CSI feedback link, sent at the beginning of each fading block, and the average power constraint in (2), an upper bound on the ergodic secrecy capacity is given by

$$\mathcal{C}_{\mathrm{s}}^{+}=\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q,\boldsymbol{\rho}_q\}}\mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}},\mathbf{H}_{\mathrm{R}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}\left[\left\{\log\frac{\left|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}}+\frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{E}}^*\right|}\right\}^{+}\right]P_q, \tag{5}$$

where $Q{=}2^B$, $\mathrm{tr}\left[\mathbb{E}[\boldsymbol{\rho}_q]\right]\leq P_{\mathrm{avg}}$, $\boldsymbol{\rho}_q\succeq 0$, and $P_q{=}\Pr\left[\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q\right]$ for all $q\in\{1,\cdots,Q\}$.

Proof: The proof is provided in the following section. We can see that the expression of the upper bound, in Theorem 2, is quite similar to the expression of $\mathcal{C}_{\mathrm{s}}^{-}$, in Theorem 1. The difference is that, for the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$, in the numerator, we have a minimization over all channels in each partition, whereas, in the upper bound, there is no such a minimization. The minimization, in the achievable secrecy rate, is required to ensure reliability as the transmitter has a limited knowledge of the main CSI. Letting Q goes to ∞, the lower bound in (3) and the upper bound in (5) coincide, hence, fully characterizing the ergodic secrecy capacity in this case.

Corollary 1: The ergodic secrecy capacity of a discrete-time memoryless multiple-antenna wiretap block fading channel with perfect main CSIT, and the average power constraint in (2), is given by

$$\mathcal{C}_{\mathrm{s}}=\max_{\boldsymbol{\rho}(\mathbf{H}_{\mathrm{R}})}\mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}},\mathbf{H}_{\mathrm{R}}}\left[\left\{\log\frac{\left|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}(\mathbf{H}_{\mathrm{R}})\mathbf{H}_{\mathrm{R}}^*\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}}+\frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\boldsymbol{\rho}(\mathbf{H}_{\mathrm{R}})\mathbf{H}_{\mathrm{E}}^*\right|}\right\}^{+}\right], \tag{6}$$

where $\mathrm{tr}\left[\mathbb{E}[\boldsymbol{\rho}(\mathbf{H}_{\mathrm{R}})]\right]\leq P_{\mathrm{avg}}$ and $\boldsymbol{\rho}(\mathbf{H}_{\mathrm{R}})\succeq 0$.

Proof: Corollary 1 results directly from the expressions of the achievable rate in (3) and the upper bound in (5), by taking into consideration that as $Q\to\infty$, the set of partition regions becomes infinite and the legitimate receiver is basically forwarding matrix $\mathbf{H}_{\mathrm{R}}$ to the transmitter.

To the best of our knowledge, this result has not been reported in earlier works. For the special case of $N_{\mathrm{T}}{=}N_{\mathrm{R}}{=}N_{\mathrm{E}}{=}1$, $\mathcal{C}_{\mathrm{s}}$ in corollary 1 coincides with the result in [4, Theorem 2].

B. Asymptotic Analysis in the High-SNR Regime

1) Finite CSI Feedback:

Corollary 2: In the high-SNR regime, the ergodic secrecy capacity $\mathcal{C}_{\mathrm{s}}^{\mathrm{FF}}$ of the discrete-time memoryless multiple-antenna wiretap channel, with finite CSI feedback, can be characterized as follows

$$\lim_{P_{\mathrm{avg}}\to\infty}\left[\mathcal{C}_{\mathrm{s}}^{\mathrm{FF}}-\{r_{\mathrm{R}}-r_{\mathrm{E}}\}^{+}\log\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}}\right]=\theta_1, \tag{7}$$

with

$$\begin{cases}\displaystyle\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q\}}\mathop{\mathbb{E}}_{\substack{\boldsymbol{\lambda}_{\mathrm{E}}|\\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}}\left[\min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}}\\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}}\sum_{i=1}^{r_{\mathrm{R}}}\log\frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2}-\sum_{i=1}^{r_{\mathrm{E}}}\log\frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2}\right]P_q\leq\theta_1 & \text{if } r_{\mathrm{R}}\geq r_{\mathrm{E}}\\ \theta_1=0 & \text{otherwise}\end{cases},$$

and where $r_{\mathrm{R}}{=}\min(N_{\mathrm{T}},N_{\mathrm{R}})$, $r_{\mathrm{E}}{=}\min(N_{\mathrm{T}},N_{\mathrm{E}})$, and $\boldsymbol{\lambda}_{\mathrm{R}}$ and $\boldsymbol{\lambda}_{\mathrm{E}}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_{\mathrm{R}}\mathbf{H}_{\mathrm{R}}^*$ and $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^*$, i.e., $\boldsymbol{\lambda}_{\mathrm{R}}{=}\{\lambda_{\mathrm{R}_1},\cdots,\lambda_{\mathrm{R}_{r_{\mathrm{R}}}}\}$ and $\boldsymbol{\lambda}_{\mathrm{E}}{=}\{\lambda_{\mathrm{E}_1},\cdots,\lambda_{\mathrm{E}_{r_{\mathrm{E}}}}\}$.

Proof: The proof is provided in Appendix A. We note that the lower bound on θ_1 is obtained by considering uniform power allocation over all transmit antennas. For the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$, uniform power allocation is nearly optimal when $N_{\mathrm{T}}{\leq}N_{\mathrm{R}}$. When $N_{\mathrm{T}}{>}N_{\mathrm{R}}$, using all transmit antennas to send the secret information is not the best that the transmitter can do. In this latter case, to transmit with fixed power, the transmitter may consider sending its confidential message over N_{T} antennas and exploits the remaining $N_{\mathrm{T}}{-}N_{\mathrm{R}}$ antennas to send artificial noise. This is, however, not easy to accomplish as the transmitter has limited knowledge of the main CSI and will end up disrupting not only to the eavesdropper but also to the legitimate receiver, especially when Q is small.

A figure-of-merit of interest is the so-called secrecy degree of freedom (SDoF) which has the same intuitive interpretation as the degree of freedom (DoF) widely used in the MIMO literature, but incorporates the secrecy constraint. Essentially, the SDoF is formally defined as

$$d_{\mathrm{s}}=\lim_{P_{\mathrm{avg}}\to\infty}\frac{\mathcal{C}_{\mathrm{s}}}{\log\left(P_{\mathrm{avg}}\right)}.$$

Theorem 3: The SDoF of the discrete-time memoryless multiple-antenna block-fading wiretap channel with finite CSI feedback is lower bounded as

$$d_{\mathrm{s}}^{\mathrm{FF}}\geq\left\{\min(N_{\mathrm{T}},N_{\mathrm{R}})-\min(N_{\mathrm{T}},N_{\mathrm{E}})\right\}^{+}.$$

Proof: The result can be deduced directly from Corollary 2. An upper bound on $d_{\mathrm{s}}^{\mathrm{FF}}$ is the SDoF with infinite CSI feedback that is characterized in the following subsection.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

2) Perfect Main CSIT:

Corollary 3: In the high-SNR regime, the ergodic secrecy capacity $\mathcal{C}_\mathrm{s}$ of the discrete-time memoryless multiple-antenna wiretap channel, with perfect main CSI, can be characterized as follows

$$\lim_{P_\mathrm{avg}\to\infty}\left[\mathcal{C}_\mathrm{s}-\min\Big(\left\{N_\mathrm{T}-N_\mathrm{E}\right\}^+,N_\mathrm{R}\Big)\log\frac{P_\mathrm{avg}}{N_\mathrm{T}}\right]=\theta_2 \tag{8}$$

with $\theta_2\le\sum_{j:\alpha_j\ge1}\log\alpha_j^2-o(1)$, and

$$\theta_2\ge\begin{cases}0 & \text{if } N_\mathrm{T}<N_\mathrm{E}\\ \mathbb{E}_{\boldsymbol{\lambda}_\mathrm{R},\boldsymbol{\lambda}_\mathrm{E}}\left[\sum_{i=1}^{N_\mathrm{T}}\log\frac{\lambda_{\mathrm{R}_i}}{\sigma_\mathrm{R}^2}-\sum_{i=1}^{N_\mathrm{E}}\log\frac{\lambda_{\mathrm{E}_i}}{\sigma_\mathrm{E}^2}\right] & \text{if } N_\mathrm{E}\le N_\mathrm{T}\le N_\mathrm{R}\\ \mathbb{E}_{\substack{\boldsymbol{\lambda}_\mathrm{R},\boldsymbol{\lambda}_\mathrm{EZ},\\ \boldsymbol{\lambda}_\mathrm{sum}}}\left[\sum_{i=1}^{N_\mathrm{R}}\log\frac{\lambda_{\mathrm{R}_i}}{\sigma_\mathrm{R}^2}+\sum_{i=1}^{\min(N_\mathrm{T}-N_\mathrm{R},N_\mathrm{E})}\log\frac{\lambda_{\mathrm{EZ}_i}}{\sigma_\mathrm{E}^2}-\sum_{i=1}^{N_\mathrm{E}}\log\frac{\lambda_{\mathrm{sum}_i}}{\sigma_\mathrm{E}^2}\right] & \text{if } N_\mathrm{T}>\max(N_\mathrm{E},N_\mathrm{R})\end{cases}, \tag{9}$$

where $\boldsymbol{\lambda}_\mathrm{R}$, $\boldsymbol{\lambda}_\mathrm{E}$, $\boldsymbol{\lambda}_\mathrm{EZ}$ and $\boldsymbol{\lambda}_\mathrm{sum}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_\mathrm{R}\mathbf{H}_\mathrm{R}^*$, $\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{E}^*$, $\mathbf{H}_\mathrm{E}\mathbf{Z}\mathbf{Z}^*\mathbf{H}_\mathrm{E}^*$ and $(\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{E}^*+\mathbf{H}_\mathrm{E}\mathbf{Z}\mathbf{Z}^*\mathbf{H}_\mathrm{E}^*)$, i.e., $\boldsymbol{\lambda}_\mathrm{R}=\{\lambda_{\mathrm{R}_1},\cdots,\lambda_{\mathrm{R}_{r_\mathrm{R}}}\}$, $\boldsymbol{\lambda}_\mathrm{E}=\{\lambda_{\mathrm{E}_1},\cdots,\lambda_{\mathrm{E}_{r_\mathrm{E}}}\}$, $\boldsymbol{\lambda}_\mathrm{EZ}=\{\lambda_{\mathrm{EZ}_1},\cdots,\lambda_{\mathrm{EZ}_{r_\mathrm{EZ}}}\}$ and $\boldsymbol{\lambda}_\mathrm{sum}=\{\lambda_{\mathrm{sum}_1},\cdots,\lambda_{\mathrm{sum}_{r_\mathrm{sum}}}\}$, with $\mathbf{Z}=\mathrm{null}(\mathbf{H}_\mathrm{R})$, the α_js represent the generalized singular values of $(\mathbf{H}_\mathrm{R},\mathbf{H}_\mathrm{E})$, and $o(1)$ is a vanishing term, i.e., $o(1)\to0$.

Proof: The proof is provided in Appendix B. Since the entries of the channel gain matrices $\mathbf{H}_\mathrm{R}$ and $\mathbf{H}_\mathrm{E}$ have bounded distributions, the constant term θ_2 is finite and does not scale with P_avg. Also, it must be emphasized that the lower bound on θ_2, when $N_\mathrm{E}\le N_\mathrm{T}\le N_\mathrm{R}$, is obtained by considering uniform power allocation over all transmit antennas. In the case when the number of transmit antennas is larger than the number of receive antennas, transmitting the secret information, solely, is no longer near optimal as the null space of $\mathbf{H}_\mathrm{R}$ becomes non-trivial. In this case, we consider the transmission of artificial noise over the null space of $\mathbf{H}_\mathrm{R}$.

Theorem 4: The SDoF of the discrete-time memoryless multiple-antenna block-fading wiretap channel with perfect main CSI is given by

$$d_\mathrm{s}=\min(\left\{N_\mathrm{T}-N_\mathrm{E}\right\}^+,N_\mathrm{R}).$$

Proof: The result can be deduced directly from Corollary 3.

Note that even thought in our case the transmitter is not aware of the eavesdropper's instantaneous CSI, the obtained SDoF are the same as if the transmitter has a perfect knowledge of both the legitimate receiver's and the eavesdropper's CSI [15].

Corollary 4: In the high-SNR regime, and with uniform power allocation over all transmit antennas, the gap between the ergodic secrecy capacity with perfect main CSI and the achievable secrecy rates with finite CSI feedback can be characterized as follows

$$\lim_{P_\mathrm{avg}\to\infty}\left[\mathcal{C}_\mathrm{s}-\mathcal{C}_\mathrm{s}^-\right]= \tag{10}$$
$$\mathbb{E}_{\boldsymbol{\lambda}_\mathrm{R}}\left[\sum_{i=1}^{N_\mathrm{T}}\log\lambda_{\mathrm{R}_i}-\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q\}}\min_{\substack{\boldsymbol{\lambda}_\mathrm{R}\\ \mathbf{H}_\mathrm{R}\in\mathcal{H}_q}}\sum_{i=1}^{N_\mathrm{T}}\log\lambda_{\mathrm{R}_i}P_q\right],$$

and

$$\lim_{P_\mathrm{avg}\to\infty}\left[\mathcal{C}_\mathrm{s}-\widetilde{\mathcal{C}}_\mathrm{s}^-\right]= \tag{11}$$
$$\mathbb{E}_{\boldsymbol{\lambda}_\mathrm{R},\boldsymbol{\lambda}_\mathrm{E}}\left[\left\{(r_\mathrm{E}-N_\mathrm{T})\log\frac{P_\mathrm{avg}}{N_\mathrm{T}}+\sum_{i=1}^{r_\mathrm{E}}\log\frac{\lambda_{\mathrm{E}_i}}{\sigma_\mathrm{E}^2}-\sum_{i=1}^{N_\mathrm{T}}\log\frac{\lambda_{\mathrm{R}_i}}{\sigma_\mathrm{R}^2}\right\}^+\right],$$

with $N_\mathrm{T}\le N_\mathrm{R}$, $r_\mathrm{E}=\min(N_\mathrm{T},N_\mathrm{E})$, and $\boldsymbol{\lambda}_\mathrm{R}$ and $\boldsymbol{\lambda}_\mathrm{E}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_\mathrm{R}\mathbf{H}_\mathrm{R}^*$ and $\mathbf{H}_\mathrm{E}\mathbf{H}_\mathrm{E}^*$, i.e., $\boldsymbol{\lambda}_\mathrm{R}=\{\lambda_{\mathrm{R}_1},\cdots,\lambda_{\mathrm{R}_{r_\mathrm{R}}}\}$ and $\boldsymbol{\lambda}_\mathrm{E}=\{\lambda_{\mathrm{E}_1},\cdots,\lambda_{\mathrm{E}_{r_\mathrm{E}}}\}$.

Proof: The proof is provided in Appendix C. It is worth mentioning that, on one hand, the asymptotic gap between $\mathcal{C}_\mathrm{s}$ and $\mathcal{C}_\mathrm{s}^-$ vanishes as the number of feedback bits increases, i.e., $Q\to\infty$. Indeed, we have

$$\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q\}}\min_{\substack{\boldsymbol{\lambda}_\mathrm{R}\\ \mathbf{H}_\mathrm{R}\in\mathcal{H}_q}}\sum_{i=1}^{N_\mathrm{T}}\log\lambda_{\mathrm{R}_i}P_q\xrightarrow[Q\to\infty]{}\sum_{i=1}^{N_\mathrm{T}}\log\lambda_{\mathrm{R}_i}.$$

On the other hand, the asymptotic gap between $\mathcal{C}_\mathrm{s}$ and $\widetilde{\mathcal{C}}_\mathrm{s}^-$ is independent of the number of feedback bits. A similar inference can be made in the case of $N_\mathrm{T}>N_\mathrm{R}$.

Remark 1: From the asymptotic expressions of the ergodic secrecy rates $\mathcal{C}_s^-$ and $\widetilde{\mathcal{C}}_s^-$, i.e.,

$$\mathcal{C}_\text{H-SNR}^-=\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q\}}\mathbb{E}_{\boldsymbol{\lambda}_\mathrm{E}|\mathbf{H}_\mathrm{R}\in\mathcal{H}_q}\left[\left\{(r_\mathrm{R}-r_\mathrm{E})\log\frac{P_\mathrm{avg}}{N_\mathrm{T}}+\min_{\substack{\boldsymbol{\lambda}_\mathrm{R}\\ \mathbf{H}_\mathrm{R}\in\mathcal{H}_q}}\sum_{i=1}^{r_\mathrm{R}}\log\frac{\lambda_{\mathrm{R}_i}}{\sigma_\mathrm{R}^2}-\sum_{i=1}^{r_\mathrm{E}}\log\frac{\lambda_{\mathrm{E}_i}}{\sigma_\mathrm{E}^2}\right\}^+\right]P_q+o\left(P_\mathrm{avg}\right), \tag{12}$$

and

$$\widetilde{\mathcal{C}}_\text{H-SNR}^-=\mathbb{E}_{\boldsymbol{\lambda}_\mathrm{R},\boldsymbol{\lambda}_\mathrm{E}}\left[(r_\mathrm{R}-r_\mathrm{E})\log\frac{P_\mathrm{avg}}{N_\mathrm{T}}+\sum_{i=1}^{r_\mathrm{R}}\log\frac{\lambda_{\mathrm{R}_i}}{\sigma_\mathrm{R}^2}-\sum_{i=1}^{r_\mathrm{E}}\log\frac{\lambda_{\mathrm{E}_i}}{\sigma_\mathrm{E}^2}\right]+o\left(P_\mathrm{avg}\right), \tag{13}$$

we can see that $\mathcal{C}_\text{H-SNR}^-$ depends on Q while $\widetilde{\mathcal{C}}_\text{H-SNR}^-$ does not. That is, when the number of antennas at the eavesdropper is less than the number of antennas at the legitimate receiver, i.e., $N_\mathrm{E}<N_\mathrm{R}$, we get $(r_\mathrm{R}-r_\mathrm{E})\ge0$, and the term inside the expectation in (12) is more likely to be positive. Then, the (+) in (12) is inactive, and because of the min in (12), (13) is clearly higher unless the number of partitions is infinitely high corresponding to the infinite-capacity feedback link. This corresponds to what we observed in Figures 3 and 4 in the manuscript.

C. Optimal Framework for Feedback and Transmission (OFFT)

1) OFFT for $\widetilde{\mathcal{C}}_s^-$: Finding the optimal feedback strategy, $\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$, and the optimal transmission strategy, $\{\boldsymbol{\rho}_1,\cdots,\boldsymbol{\rho}_Q\}$, that maximizes the achievable secrecy rate $\widetilde{\mathcal{C}}_\mathrm{s}^-$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

in (4), is equivalent to the design of a vector quantizer with a modified distortion measure. Let λ be the Lagrange multiplier corresponding to the average transmit power constraint. We define the following distortion measure

$$\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_q\right)=-\left[\log\frac{\left|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}}+\frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{E}}^*\right|}-\lambda\mathrm{tr}\boldsymbol{\rho}_q\right], \tag{14}$$

where $\boldsymbol{\rho}_q\succeq 0$ and $q=\{1,\cdots,Q\}$. We need to find the optimal $\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$ and $\{\boldsymbol{\rho}_1,\cdots,\boldsymbol{\rho}_Q\}$ that minimizes the average distortion measure $\widetilde{\Delta}$ given by

$$\widetilde{\Delta}=\sum_{q=1}^{Q}\mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}},\mathbf{H}_{\mathrm{R}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}\left[\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_q\right)\right]P_q.$$

To solve this optimization problem, we use Lloyd's algorithm [43]. The OFFT for the achievable secrecy rate $\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}$ is given in Algo.1[1]. It should be noted that since we are using Lloyd algorithm, the partitioning is performed according to the Voronoi diagram using the nearest neighbor rule, i.e.,

$$\mathcal{H}_q=\left\{\mathbf{H}_{\mathrm{R}}:\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_q\right)\leq\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_j\right);\forall j\neq q\right\}.$$

The probability P_q can then be characterized, in this case, as follows

$$\begin{aligned}P_q&=\Pr\left[\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q\right]\\&=\Pr\left[\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_q\right)\leq\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_j\right);\forall j\neq q\right]\\&=\Pr\left[\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_q\right)\leq\max_{j\in\{1,\cdots,Q\},j\neq q}\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_j\right)\right].\end{aligned}$$

We should also mention that the proposed scheme is an offline optimization algorithm and it only depends on the knowledge of the statistics of the channel gains, not on the actual instantaneous channel realizations.

2) OFFT for $\mathcal{C}_s^-$: To design the optimal feedback and transmission codebooks that maximizes the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$ in (3), we consider the following modified distortion measure

$$\delta\left(\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_q\right)=-\left[\left\{\log\frac{\left|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}}+\frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{E}}^*\right|}\right\}^{+}-\lambda\mathrm{tr}\boldsymbol{\rho}_q\right], \tag{15}$$

where $\boldsymbol{\rho}_q\succeq 0$, $q=\{1,\cdots,Q\}$ and λ is the Lagrange multiplier. We need to find the optimal $\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$ and $\{\boldsymbol{\rho}_1,\cdots,\boldsymbol{\rho}_Q\}$ that minimizes the average distortion measure

$$\Delta=\sum_{q=1}^{Q}\mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}\left[\delta\left(\mathbf{T}_q,\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_q\right)\right]P_q,$$

where $\mathbf{T}_q=\mathop{\arg\min}_{\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}\left|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|$.

To solve this optimization problem, we use Lloyd's algorithm [43]. The OFFT for the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$ is given in Algo.2.

[1]In general, there is no guarantee that Lloyd's algorithm converges to the global optimum [43]. In the simulations, we repeat the iterations multiple times and pick the one that gives us the largest secrecy rate.

Algorithm 1: OFFT for $\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}$

Input : Q, λ.
Output: Optimal feedback and transmission strategy $\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$ and $\{\boldsymbol{\rho}_1,\cdots,\boldsymbol{\rho}_Q\}$.
Consider a random partition of the space of $\mathbf{H}_{\mathrm{R}}$: $\mathbb{H}_1=\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$;
Define $\mathbb{H}_0$ as the set of Q empty regions;
Let $itr=1$;
while $\mathbb{H}_{itr}\neq\mathbb{H}_{itr-1}$ **do**
  for $q=1:Q$ **do**
    Find the optimal transmission strategy $\boldsymbol{\rho}_q$, given by the *generalized partition centroid*:
    $\boldsymbol{\rho}_q=\arg\min_{\boldsymbol{\rho}_q}\mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}},\mathbf{H}_{\mathrm{R}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}\left[\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_q\right)\right]P_q$;
  for $q=1:Q$ **do**
    Find the optimal partition region $\mathcal{H}_q$, given the transmission strategies $\{\boldsymbol{\rho}_1,\cdots,\boldsymbol{\rho}_Q\}$, using the *nearest neighbor rule*:
    $\mathcal{H}_q=\Big\{\mathbf{H}_{\mathrm{R}}:\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_q\right)\leq\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}},\boldsymbol{\rho}_j\right);\ \forall j\in\{1,\cdots,Q\},j\neq q\Big\}$;
  $itr=itr+1$;
  $\mathbb{H}_{itr}=\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$;
$P_{\mathrm{avg}}=\sum_{q=1}^{Q}\mathrm{tr}\boldsymbol{\rho}_q\Pr\left[\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q\right]$.

IV. Ergodic Capacity Analysis

In this section, we establish the lower and the upper bounds on the ergodic secrecy capacity presented in Theorem 1 and Theorem 2, respectively.

A. Proof of Achievability in Theorem 1

1) Proof of the Lower Bound $\mathcal{C}_s^-$: Given a partition of the channel gain space $\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$ and a transmission strategy $\{\boldsymbol{\rho}_1,\cdots,\boldsymbol{\rho}_Q\}$, let $\mathbf{T}_q$, $q\in\{1,\cdots,Q\}$, be the element of $\mathcal{H}_q$ that minimizes the function $\xi(\mathbf{H}_{\mathrm{R}})=\left|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|$, i.e.,

$$\left|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{T}_q\boldsymbol{\rho}_q\mathbf{T}_q^*\right|\leq\left|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|,$$

for all $\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q$. We note that such a minimum exists since the function $\xi(\mathbf{H}_{\mathrm{R}})$ is logarithmically concave in $\mathbf{H}_{\mathrm{R}}$, and $\mathcal{H}_q$ corresponds to a Voronoi region which is by definition a convex set [46]. We assume that the rates

$$R_q=\log\left|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{T}_q\boldsymbol{\rho}_q\mathbf{T}_q^*\right|,$$

are selected in advance. We need to prove that the rate

$$R_{\mathrm{s}}^{-}=\sum_{q=1}^{Q}P_q\mathop{\mathbb{E}}_{\substack{\mathbf{H}_{\mathrm{E}}|\\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}}\left[\left\{R_q-\log\left|\mathbf{I}_{N_{\mathrm{E}}}+\frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{E}}^*\right|\right\}^{+}\right]-\epsilon_1, \tag{16}$$

is achievable.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

Algorithm 2: OFFT for $\mathcal{C}_{\rm s}^-$

Input : Q, λ.
Output: Optimal feedback and transmission strategy $\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$ and $\{\boldsymbol{\rho}_1,\cdots,\boldsymbol{\rho}_Q\}$.
Consider a random partition of the space of $\mathbf{H}_{\rm R}$: $\mathbb{H}_1=\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$;
Define $\mathbb{H}_0$ as the set of Q empty regions;
Let $itr=1$;
while $\mathbb{H}_{itr}\neq\mathbb{H}_{itr-1}$ **do**
  for $q=1:Q$ **do**
    $\mathbf{T}_q(\boldsymbol{\rho}_q)=\underset{\mathbf{H}_{\rm R}\in\mathcal{H}_q}{\arg\min}\left|\mathbf{I}_{N_{\rm R}}+\frac{1}{\sigma_{\rm R}^2}\mathbf{H}_{\rm R}\boldsymbol{\rho}_q\mathbf{H}_{\rm R}^*\right|$;
    Find the optimal transmission strategy:
    $\boldsymbol{\rho}_q=\arg\min_{\boldsymbol{\rho}_q}\underset{\mathbf{H}_{\rm E}|\mathbf{H}_{\rm R}\in\mathcal{H}_q}{\mathbb{E}}\left[\delta\left(\mathbf{T}_q(\boldsymbol{\rho}_q),\mathbf{H}_{\rm E},\boldsymbol{\rho}_q\right)\right]P_q$;
  for $q=1:Q$ **do**
    Find the optimal partition region:
    $\mathcal{H}_q=\Big\{\mathbf{H}_{\rm R}:\delta\left(\mathbf{H}_{\rm R},\mathbf{H}_{\rm E},\boldsymbol{\rho}_q\right)\leq\delta\left(\mathbf{H}_{\rm R},\mathbf{H}_{\rm E},\boldsymbol{\rho}_j\right);\ \forall j\in\{1,\cdots,Q\},j\neq q\Big\}$;
  $itr=itr+1$;
  $\mathbb{H}_{itr}=\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$;
$P_{\rm avg}=\sum_{q=1}^{Q}\mathrm{tr}\boldsymbol{\rho}_q\Pr\left[\mathbf{H}_{\rm R}\in\mathcal{H}_q\right]$.

Let

$$R_{\rm e}=\sum_{q=1}^{Q}P_q\underset{\mathbf{H}_{\rm E}|\mathbf{H}_{\rm R}\in\mathcal{H}_q}{\mathbb{E}}\left[\log\left|\mathbf{I}_{N_{\rm E}}+\frac{1}{\sigma_{\rm E}^2}\mathbf{H}_{\rm E}\boldsymbol{\rho}_q\mathbf{H}_{\rm E}^*\right|\right]-\epsilon_2. \quad (17)$$

The considered wiretap codebook is generated by uniformly and randomly partitioning the 2^{nR_m} length n sequences into $2^{nR_{\rm s}^-}$ bins; each containing $2^{nR_{\rm e}}$ codewords, where $R_m=\sum_{q=1}^{Q}P_qR_q-\epsilon$. That is, to transmit a message W, the transmitter selects the corresponding bin and then randomly chooses a binary sequence among all the uniformly distributed codewords in the selected bin. During each fading block, of length κ, the transmitter sends κR_q information bits using the generated Gaussian codebook. Then, using the weak law of large numbers, when the number of spanned fading blocks L is large, the entire binary sequence is transmitted with high probability. Also, since $R_q\leq\log\left|\mathbf{I}_{N_{\rm R}}+\mathbf{H}_{\rm R}\boldsymbol{\rho}_q\mathbf{H}_{\rm R}^*\right|$ is valid for all fading blocks, the receiver can decode the transmitted signal with a negligible probability of error.

For the secrecy analysis, we need to prove that the equivocation rate satisfies $R_{\rm e}\geq R_{\rm s}^--\epsilon$. We have

$$nR_{\rm e}=H(W|\mathbf{Y}_{\rm E}^n,\mathbf{H}_{\rm E}^L,\mathbf{H}_{\rm R}^L,U^L) \quad (18)$$
$$\geq I(W;\mathbf{X}^n|\mathbf{Y}_{\rm E}^n,\mathbf{H}_{\rm E}^L,\mathbf{H}_{\rm R}^L,U^L) \quad (19)$$
$$=H(\mathbf{X}^n|\mathbf{Y}_{\rm E}^n,\mathbf{H}_{\rm E}^L,\mathbf{H}_{\rm R}^L,U^L)-H(\mathbf{X}^n|\mathbf{Y}_{\rm E}^n,\mathbf{H}_{\rm E}^L,\mathbf{H}_{\rm R}^L,U^L,W). \quad (20)$$

On one hand, we can write

$$H(\mathbf{X}^n|\mathbf{Y}_{\rm E}^n,\mathbf{H}_{\rm E}^L,\mathbf{H}_{\rm R}^L,U^L)$$
$$=\sum_{l=1}^{L}H(X^\kappa(l)|\mathbf{Y}_{\rm E}^\kappa(l),\mathbf{H}_{\rm E}(l),\mathbf{H}_{\rm R}(l),U(l)) \quad (21)$$
$$\geq\sum_{l\in\mathcal{S}_L}H(X^\kappa(l)|\mathbf{Y}_{\rm E}^\kappa(l),\mathbf{H}_{\rm E}(l),\mathbf{H}_{\rm R}(l),U(l)) \quad (22)$$
$$\geq\sum_{l\in\mathcal{S}_L}\kappa\left[\sum_{q=1}^{Q}P_q\left[R_q-\log\left|\mathbf{I}_{N_{\rm E}}+\frac{1}{\sigma_{\rm E}^2}\mathbf{H}_{\rm E}(l)\boldsymbol{\rho}_q\mathbf{H}_{\rm E}^*(l)\right|\right]-\epsilon'\right] \quad (23)$$
$$=\sum_{l=1}^{L}\kappa\left[\sum_{q=1}^{Q}P_q\left\{R_q-\log\left|\mathbf{I}_{N_{\rm E}}+\frac{1}{\sigma_{\rm E}^2}\mathbf{H}_{\rm E}(l)\boldsymbol{\rho}_q\mathbf{H}_{\rm E}^*(l)\right|\right\}^+-\epsilon'\right] \quad (24)$$
$$=n\sum_{q=1}^{Q}P_q\underset{\substack{\mathbf{H}_{\rm E}|\\ \mathbf{H}_{\rm R}\in\mathcal{H}_q}}{\mathbb{E}}\left[\left\{R_q-\log\left|\mathbf{I}_{N_{\rm E}}+\frac{1}{\sigma_{\rm E}^2}\mathbf{H}_{\rm E}\boldsymbol{\rho}_q\mathbf{H}_{\rm E}^*\right|\right\}^+\right]-n\epsilon' \quad (25)$$
$$=nR_{\rm s}^--n\epsilon', \quad (26)$$

where (21) results from the memoryless property of the channel and the independence of the $X^\kappa(l)$'s, (22) is obtained by removing all the terms corresponding to the fading blocks $l\notin\mathcal{S}_L$, with $\mathcal{S}_L=\{l\in\{1,\cdots,L\}:\mathbf{T}_q(l)>\mathbf{H}_{\rm E}(l)\}$, and (25) follows from the ergodicity of the channel as $L\to\infty$.

On the other hand, using list decoding argument at the eavesdropper side and applying Fano's inequality [4], $\frac{1}{n}H(\mathbf{X}^n|\mathbf{Y}_{\rm E}^n,\mathbf{H}_{\rm E}^L,U^L,W)$ vanishes as $n\to\infty$ and we can write

$$H(\mathbf{X}^n|\mathbf{Y}_{\rm E}^n,\mathbf{H}_{\rm E}^L,\mathbf{H}_{\rm R}^L,W)\leq n\epsilon''. \quad (27)$$

Substituting (26) and (27) in (20), we get $R_{\rm e}\geq R_{\rm s}^--\epsilon$, with $\epsilon=\epsilon'+\epsilon''$, and ϵ' and ϵ'' are selected to be arbitrarily small. Maximizing over the main channel gain partition regions $\mathcal{H}_q$ and the associated transmission strategies $\boldsymbol{\rho}_q$, for each $q\in\{1,\cdots,Q\}$, concludes the proof. □

2) Proof of the Lower Bound $\widetilde{\mathcal{C}}_s^-$: In the proposed communication system, the transmitter uses the feedbacked partition index to select the optimal beamforming and power control matrices for the forward transmission. This could be seen as a deterministic mapping that associates each feedback index u_q with a beamforming matrix $\mathbf{V}_q$ and a power control matrix $\boldsymbol{\Lambda}_q$. The adopted system model, illustrated in Fig. 1, can then be equivalently modeled by the block diagram in Fig. 2. That is, the original adaptive encoding function, which produces symbol X from message W using the feedback information U, is replaced by an encoding entity and a deterministic mapping function, φ, that becomes part of the channel.

The new encoder is independent of U and uses a wiretap codebook to construct the new channel input alphabet $\mathbf{T}$ from message W, whereas the mapping function f adapts the transmission of signal $\mathbf{T}$ using U, i.e., $\varphi(u_q,\mathbf{T})=\mathbf{V}_q\boldsymbol{\Lambda}_q\mathbf{T}$. The equivalent channel model becomes a multiple-antenna memoryless channel without feedback, with input $\mathbf{T}$ and outputs $(\mathbf{Y}_{\rm R},\mathbf{H}_{\rm R},U)$ at the legitimate receiver, and $(\mathbf{Y}_{\rm E},\mathbf{H}_{\rm E},U)$ at the eavesdropper. Thus, using [47, Proposition 2] and [2, Corollary 2], the following secrecy rate is achievable $\widetilde{R}_{\rm s}^-=I(\mathbf{T};\mathbf{Y}_{\rm R}|\mathbf{H}_{\rm R},U)-I(\mathbf{T};\mathbf{Y}_{\rm E}|\mathbf{H}_{\rm E},U)$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

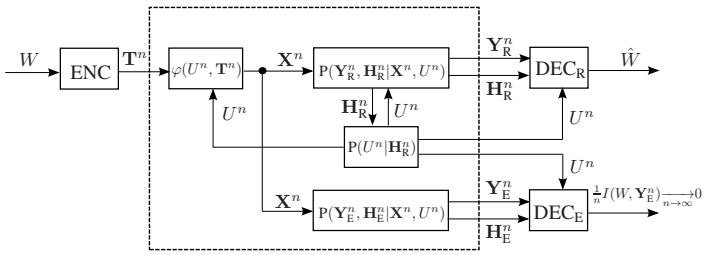

Fig. 2. Equivalent channel model of the communication system with input $\mathbf{T}^n$ and outputs $\mathbf{Y}_\mathrm{R}^n$ and $\mathbf{H}_\mathrm{R}^n$, at the legitimate receiver, and $\mathbf{Y}_\mathrm{E}^n$ and $\mathbf{H}_\mathrm{E}^n$, at the eavesdropper.

Now, since

$$I(\mathbf{T};\mathbf{Y}_\mathrm{R}|\mathbf{H}_\mathrm{R},U)=\sum_{q=1}^{Q}\mathop{\mathbb{E}}_{\mathbf{H}_\mathrm{R}\in\mathcal{H}_q}\left[I(\mathbf{T};\mathbf{Y}_\mathrm{R}|\mathbf{H}_\mathrm{R},u_q)\right]P_q,$$

and $I(\mathbf{T};\mathbf{Y}_\mathrm{E}|\mathbf{H}_\mathrm{E},U)$ can be expressed similarly, then, taking $\mathbf{T}\sim\mathcal{CN}(0,\mathbf{I}_{N_\mathrm{T}})$, the achievable secrecy rate R_s^- can be rewritten as

$$\widetilde{R}_\mathrm{s}^-=\sum_{q=1}^{Q}\left\{\mathop{\mathbb{E}}_{\mathbf{H}_\mathrm{E},\mathbf{H}_\mathrm{R}|\mathbf{H}_\mathrm{R}\in\mathcal{H}_q}\left[\log\left|\mathbf{I}_{N_\mathrm{R}}+\frac{1}{\sigma_\mathrm{R}^2}\mathbf{H}_\mathrm{R}\boldsymbol{\rho}_q\mathbf{H}_\mathrm{R}^*\right|-\log\left|\mathbf{I}_{N_\mathrm{E}}+\frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}\boldsymbol{\rho}_q\mathbf{H}_\mathrm{E}^*\right|\right]\right\}P_q. \quad (28)$$

Then, maximizing over the main channel gain partition regions $\mathcal{H}_q$ and the associated transmission strategies $\boldsymbol{\rho}_q$, for each $q\in\{1,\cdots,Q\}$, concludes the proof. □

B. Proof of the Upper Bound in Theorem 2

Let R_E be the equivocation rate at the eavesdropper. We recall that $n{=}\kappa L$, with L being the total number of spanned fading blocks and κ the length of each block. We have

$$nR_\mathrm{E}=H(W|\mathbf{Y}_\mathrm{E}^n,\mathbf{H}_\mathrm{E}^L,\mathbf{H}_\mathrm{R}^L,U^L) \quad (29)$$

$$=I(W;\mathbf{Y}_\mathrm{R}^n|\mathbf{Y}_\mathrm{E}^n,\mathbf{H}_\mathrm{E}^L,\mathbf{H}_\mathrm{R}^L,U^L)+H(W|\mathbf{Y}_\mathrm{R}^n,\mathbf{Y}_\mathrm{E}^n,\mathbf{H}_\mathrm{E}^L,\mathbf{H}_\mathrm{R}^L,U^L) \quad (30)$$

$$\le I(W;\mathbf{Y}_\mathrm{R}^n|\mathbf{Y}_\mathrm{E}^n,\mathbf{H}_\mathrm{E}^L,\mathbf{H}_\mathrm{R}^L,U^L)+n\epsilon \quad (31)$$

$$=\sum_{l=1}^{L}\sum_{k=1}^{\kappa}I(W;\mathbf{Y}_\mathrm{R}(l,k)|\mathbf{Y}_\mathrm{E}^n,\mathbf{H}_\mathrm{E}^L,\mathbf{H}_\mathrm{R}^L,U^L,\mathbf{Y}_\mathrm{R}^{\kappa(l-1)+(k-1)})+n\epsilon \quad (32)$$

$$=\sum_{l=1}^{L}\sum_{k=1}^{\kappa}H(\mathbf{Y}_\mathrm{R}(l,k)|\mathbf{Y}_\mathrm{E}^n,\mathbf{H}_\mathrm{E}^L,\mathbf{H}_\mathrm{R}^L,U^L,\mathbf{Y}_\mathrm{R}^{\kappa(l-1)+(k-1)})-H(\mathbf{Y}_\mathrm{R}(l,k)|W,\mathbf{Y}_\mathrm{E}^n,\mathbf{H}_\mathrm{E}^L,\mathbf{H}_\mathrm{R}^L,U^L,\mathbf{Y}_\mathrm{R}^{\kappa(l-1)+(k-1)})+n\epsilon \quad (33)$$

$$\le\sum_{l=1}^{L}\sum_{k=1}^{\kappa}H(\mathbf{Y}_\mathrm{R}(l,k)|\mathbf{Y}_\mathrm{E}(l,k),\mathbf{H}_\mathrm{E}(l),\mathbf{H}_\mathrm{R}(l),U^l)-H(\mathbf{Y}_\mathrm{R}(l,k)|W,X(l,k),\mathbf{Y}_\mathrm{E}^n,\mathbf{H}_\mathrm{E}^L,\mathbf{H}_\mathrm{R}^L,U^L,\mathbf{Y}_\mathrm{R}^{\kappa(l-1)+(k-1)})+n\epsilon \quad (34)$$

$$=\sum_{l=1}^{L}\sum_{k=1}^{\kappa}H(\mathbf{Y}_\mathrm{R}(l,k)|\mathbf{Y}_\mathrm{E}(l,k),\mathbf{H}_\mathrm{E}(l),\mathbf{H}_\mathrm{R}(l),U^l)-H(\mathbf{Y}_\mathrm{R}(l,k)|X(l,k),\mathbf{Y}_\mathrm{E}(l,k),\mathbf{H}_\mathrm{E}(l),\mathbf{H}_\mathrm{R}(l),U^l)+n\epsilon \quad (35)$$

$$=\sum_{l=1}^{L}\sum_{k=1}^{\kappa}I(X(l,k);\mathbf{Y}_\mathrm{R}(l,k)|\mathbf{Y}_\mathrm{E}(l,k),\mathbf{H}_\mathrm{E}(l),\mathbf{H}_\mathrm{R}(l),U^l)+n\epsilon \quad (36)$$

$$\le\sum_{l=1}^{L}\sum_{k=1}^{\kappa}\mathop{\mathbb{E}}_{\substack{\omega_l,\mathbf{H}_\mathrm{R}(l)\\ \mathbf{H}_\mathrm{E}(l),}}\left[\left\{\log\frac{|\mathbf{I}_{N_\mathrm{R}}+\frac{1}{\sigma_\mathrm{R}^2}\mathbf{H}_\mathrm{R}(l)\omega_l(U^l)\mathbf{H}_\mathrm{R}^*(l)|}{|\mathbf{I}_{N_\mathrm{E}}+\frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}(l)\omega_l(U^l)\mathbf{H}_\mathrm{E}^*(l)|}\right\}^+\right]+n\epsilon \quad (37)$$

where (31) comes from Fano's inequality, (34) follows since conditioning reduces the entropy, and (37) holds true since given $\mathbf{H}_\mathrm{R}(l)$ and $\mathbf{H}_\mathrm{E}(l)$, the channel at hand is a multiple antenna wiretap channel and, hence, the bound in (36) is tight if $\mathbf{X}^n$ is a sequence with zero-mean Gaussian components $X(l,k)$, statistically independent conditionally on U^L, i.e., $X(l,k)\sim\mathcal{CN}\left(0,\omega_l^{1/2}(U^l)\right)$, with the power policy $\omega_l(U^l)$ satisfying the average power constraint.

Since the channel gains and the feedback information are constant during each fading block, we can write

$$nR_\mathrm{E}\le\sum_{l=1}^{L}\kappa\mathop{\mathbb{E}}_{\substack{\omega_l,\mathbf{H}_\mathrm{R}(l)\\ \mathbf{H}_\mathrm{E}(l),}}\left[\left\{\log\frac{|\mathbf{I}_{N_\mathrm{R}}+\frac{1}{\sigma_\mathrm{R}^2}\mathbf{H}_\mathrm{R}(l)\omega_l(U^l)\mathbf{H}_\mathrm{R}^*(l)|}{|\mathbf{I}_{N_\mathrm{E}}+\frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}(l)\omega_l(U^l)\mathbf{H}_\mathrm{E}^*(l)|}\right\}^+\right]+n\epsilon \quad (38)$$

$$=\sum_{l=1}^{L}\kappa\mathop{\mathbb{E}}_{\substack{\omega_l,\\ \mathbf{H}_\mathrm{R}(l),\\ \mathbf{H}_\mathrm{E}(l)}}\left[\mathbb{E}\left[\left\{\log\frac{|\mathbf{I}_{N_\mathrm{R}}+\frac{1}{\sigma_\mathrm{R}^2}\mathbf{H}_\mathrm{R}(l)\omega_l(U^l)\mathbf{H}_\mathrm{R}^*(l)|}{|\mathbf{I}_{N_\mathrm{E}}+\frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}(l)\omega_l(U^l)\mathbf{H}_\mathrm{E}^*(l)|}\right\}^+\Big|U(l),\mathbf{H}_\mathrm{R}(l),\mathbf{H}_\mathrm{E}(l)\right]\right]+n\epsilon \quad (39)$$

$$\le\sum_{l=1}^{L}\kappa\mathop{\mathbb{E}}_{\substack{\omega_l,\\ \mathbf{H}_\mathrm{R}(l),\\ \mathbf{H}_\mathrm{E}(l)}}\left[\left\{\log\frac{|\mathbf{I}_{N_\mathrm{R}}+\frac{1}{\sigma_\mathrm{R}^2}\mathbf{H}_\mathrm{R}(l)\mathbb{E}[\omega_l(U^l)|U(l),\mathbf{H}_\mathrm{R}(l),\mathbf{H}_\mathrm{E}(l)]\,\mathbf{H}_\mathrm{R}^*(l)|}{|\mathbf{I}_{N_\mathrm{E}}+\frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}(l)\mathbb{E}[\omega_l(U^l)|U(l),\mathbf{H}_\mathrm{R}(l),\mathbf{H}_\mathrm{E}(l)]\,\mathbf{H}_\mathrm{E}^*(l)|}\right\}^+\right]+n\epsilon \quad (40)$$

$$=\sum_{l=1}^{L}\kappa\mathop{\mathbb{E}}_{\substack{\Omega_l,\\ \mathbf{H}_\mathrm{R}(l),\\ \mathbf{H}_\mathrm{E}(l)}}\left[\left\{\log\frac{|\mathbf{I}_{N_\mathrm{R}}+\frac{1}{\sigma_\mathrm{R}^2}\mathbf{H}_\mathrm{R}(l)\Omega_l(U(l))\mathbf{H}_\mathrm{R}^*(l)|}{|\mathbf{I}_{N_\mathrm{E}}+\frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}(l)\Omega_l(U(l))\mathbf{H}_\mathrm{E}^*(l)|}\right\}^+\right]+n\epsilon \quad (41)$$

$$=\sum_{l=1}^{L}\kappa\mathop{\mathbb{E}}_{\Omega_l,\mathbf{H}_\mathrm{R},\mathbf{H}_\mathrm{E}}\left[\left\{\log\frac{|\mathbf{I}_{N_\mathrm{R}}+\frac{1}{\sigma_\mathrm{R}^2}\mathbf{H}_\mathrm{R}\Omega_l(U)\mathbf{H}_\mathrm{R}^*|}{|\mathbf{I}_{N_\mathrm{E}}+\frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}\Omega_l(U)\mathbf{H}_\mathrm{E}^*|}\right\}^+\right]+n\epsilon, \quad (42)$$

where (40) is obtained by using Jensen's inequality since the function $X\to\left\{\log\frac{|\mathbf{I}+\mathbf{A}\mathbf{X}\mathbf{A}^*|}{|\mathbf{I}+\mathbf{B}\mathbf{X}\mathbf{B}^*|}\right\}^+$ is concave over the set of nonnegative definite matrices, $\Omega_l(U(l))$ in (41) is defined as

$$\Omega_l(U(l))=\mathbb{E}\left[\omega_l(U^l)|U(l)\right],$$

since given $U(l)$, U^l is independent of $\mathbf{H}_\mathrm{R}(l)$ and $\mathbf{H}_\mathrm{E}(l)$, and where (42) follows from the ergodicity and the stationarity of the channel gains, i.e., the expectation in (41) does not depend on the block fading index. Thus, we have

$$R_\mathrm{E}\le\frac{1}{L}\sum_{l=1}^{L}\mathop{\mathbb{E}}_{\Omega_l,\mathbf{H}_\mathrm{R},\mathbf{H}_\mathrm{E}}\left[\left\{\log\frac{|\mathbf{I}_{N_\mathrm{R}}+\frac{1}{\sigma_\mathrm{R}^2}\mathbf{H}_\mathrm{R}\Omega_l(U)\mathbf{H}_\mathrm{R}^*|}{|\mathbf{I}_{N_\mathrm{E}}+\frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}\Omega_l(U)\mathbf{H}_\mathrm{E}^*|}\right\}^+\right]+\epsilon \quad (43)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

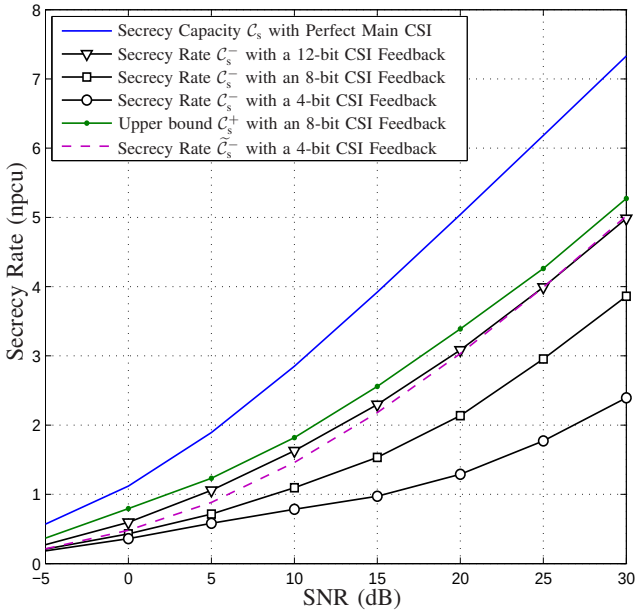

Fig. 3. Achievable secrecy rates for i.i.d. Rayleigh fading channels with $N_{\mathrm{T}}{=}N_{\mathrm{R}}{=}2$, $N_{\mathrm{E}}{=}1$ and various B-bit CSI feedback, $B{=}4, 8, 12$.

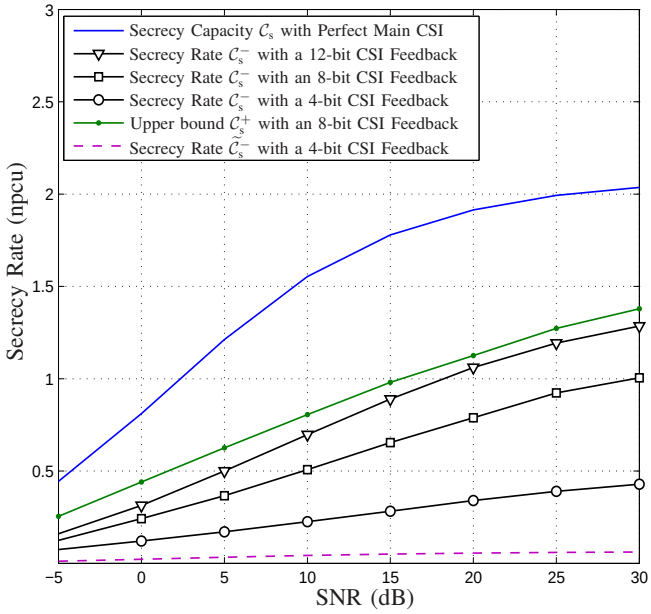

Fig. 4. Achievable secrecy rates for i.i.d. Rayleigh fading channels with $N_{\mathrm{T}}{=}N_{\mathrm{R}}{=}N_{\mathrm{E}}{=}2$ and various B-bit CSI feedback, $B{=}4, 8, 12$.

$$\leq \mathop{\mathbb{E}}_{\Omega_l,\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}}}\left[\left\{\log\frac{\left|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\frac{1}{L}\sum_{l=1}^{L}\Omega_l(U)\mathbf{H}_{\mathrm{R}}^*\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}}+\frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\frac{1}{L}\sum_{l=1}^{L}\Omega_l(U)\mathbf{H}_{\mathrm{E}}^*\right|}\right\}^+\right]+\epsilon \quad (44)$$

$$= \mathop{\mathbb{E}}_{\Omega,\mathbf{H}_{\mathrm{R}},\mathbf{H}_{\mathrm{E}}}\left[\left\{\log\frac{|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\Omega(U)\mathbf{H}_{\mathrm{R}}^*|}{|\mathbf{I}_{N_{\mathrm{E}}}+\frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\Omega(U)\mathbf{H}_{\mathrm{E}}^*|}\right\}^+\right]+\epsilon, \quad (45)$$

where (44) comes from applying Jensen's inequality once again, and where $\Omega(U)$ in (45) is defined as $\Omega(U){=}\sum_{l=1}^{L}\Omega_l(U)$. Maximizing over the main channel gain partition regions $\mathcal{H}_q$ and the associated transmission strategies $\boldsymbol{\rho}_q$, for each $q \in \{1, \cdots, Q\}$, concludes the proof. □

V. Simulation Results

In this section, we provide selected simulation results for the case of independent and identically distributed Rayleigh fading channels. We consider that the system's variables, the entries of the main channel gain matrix $\mathbf{H}_{\mathrm{R}}$ and the eavesdropper's channel gain matrix $\mathbf{H}_{\mathrm{E}}$, are all drawn from the zero-mean, unit-variance Gaussian distribution, with a number of realizations equal to 10^4.

Figure 3 and Figure 4 illustrate the achievable secrecy rates $\mathcal{C}_{\mathrm{s}}^-$ and $\widetilde{\mathcal{C}}_{\mathrm{s}}^-$, in nats per channel use (npcu), when the transmitter and the legitimate receiver have two antennas each, i.e. $N_{\mathrm{T}}{=}N_{\mathrm{R}}{=}2$. The eavesdropper is equipped with one antenna in Figure 3, i.e., $N_{\mathrm{E}}{=}1$, and with two antennas in Figure 4, i.e., $N_{\mathrm{E}}{=}2$. The upper bound $\mathcal{C}_{\mathrm{s}}^+$ and the ergodic secrecy capacity $\mathcal{C}_{\mathrm{s}}$, from Corollary 1, are also presented in both figures. On one hand, we can see, from both figures, that as the capacity of the feedback link grows, i.e., the number of bits B increases, the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^-$ grows toward the secrecy capacity $\mathcal{C}_{\mathrm{s}}$. On the other hand, we can observe that the secrecy rate $\widetilde{\mathcal{C}}_{\mathrm{s}}^-$, in Figure 3, is almost comparable to the secrecy rate $\mathcal{C}_{\mathrm{s}}^-$ with 12 bits CSI feedback; while, in Figure 4, $\widetilde{\mathcal{C}}_{\mathrm{s}}^-$ is very low even compared to $\mathcal{C}_{\mathrm{s}}^-$ with 4 bits CSI feedback. We should mention that, in both figures, we illustrate the achievable secrecy rate $\widetilde{\mathcal{C}}_s^-$ only for the case when $B = 4$. The reason behind this is that, through the conducted simulations, we noticed that increasing the number of feedback bits has a limited impact on $\widetilde{\mathcal{C}}_s^-$ compared to $\mathcal{C}_s^-$. Indeed, increasing B only results in a slight improvement of $\widetilde{\mathcal{C}}_s^-$, and only at very low SNR values where the achieved secrecy rates are small, making this improvement insignificant. The secrecy rate $\widetilde{\mathcal{C}}_{\mathrm{s}}^-$ is more convenient when the number of antennas at the eavesdropper is less than the number of antennas at the legitimate receiver, and the number of CSI feedback bits is small, which is in perfect agreement with Corollary 4 and Remark 1.

In Figure 5, the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^-$ is presented along with the secrecy capacity $\mathcal{C}_{\mathrm{s}}$ when both the transmitter and the legitimate receiver have two antennas each, i.e. $N_{\mathrm{T}}{=}N_{\mathrm{R}}{=}2$, and twelve bits are used for CSI feedback, i.e. $B{=}12$. The figure compares the cases when the eavesdropper has only one antenna, i.e. $N_{\mathrm{E}}{=}1$ and when he has two antennas, i.e. $N_{\mathrm{E}}{=}2$. As expected, the secrecy rate is higher when the eavesdropper has fewer antennas compared to the transmitter and the legitimate receiver.

The effect of changing the number of antennas, at the legitimate receiver, is illustrated in Figure 6 when 8 bits are used for CSI feedback, $N_{\mathrm{T}}{=}2$, $N_{\mathrm{E}}{=}1$, and N_{R} varies between one and four antennas. Clearly, we can see that as we augment the number of antennas at the legitimate receiver, the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^-$ increases. Also, we can notice that when the legitimate receiver has an equal number of antennas

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

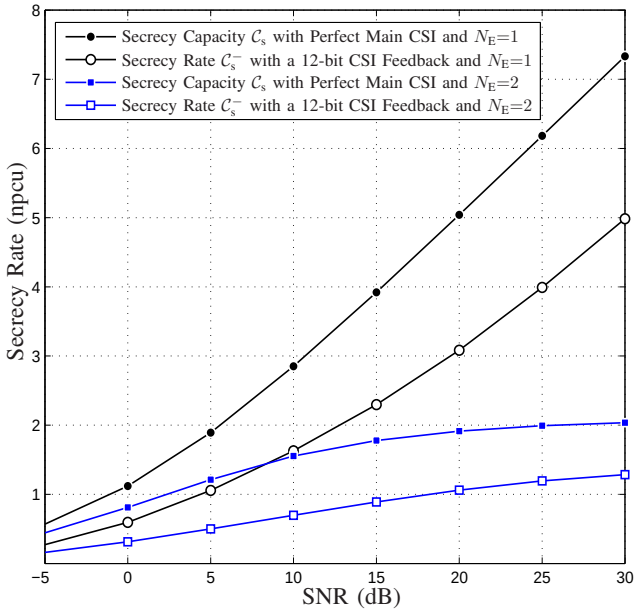

Fig. 5. Comparison of the achievable secrecy rates when the eavesdropper has one and two antennas with N_T=N_R=2 and 12 bits feedback.

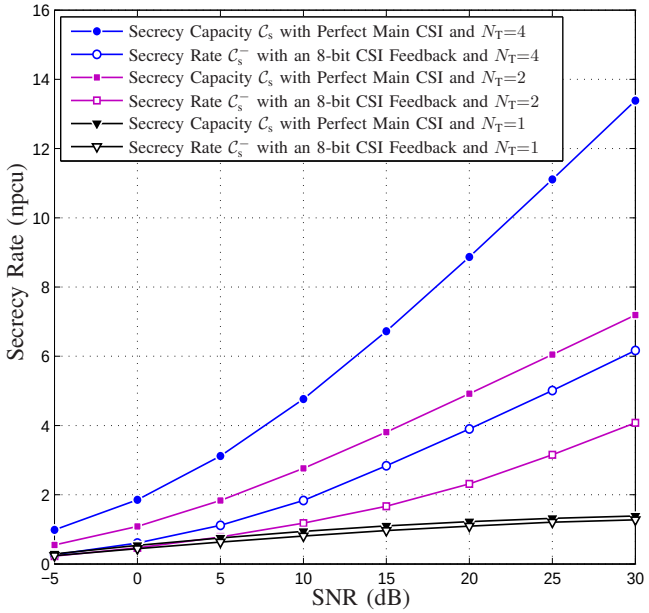

Fig. 7. Comparison of the achievable secrecy rates when the transmitter has one, two, and four antennas with N_R=2, N_E=1 and 8 bits feedback.

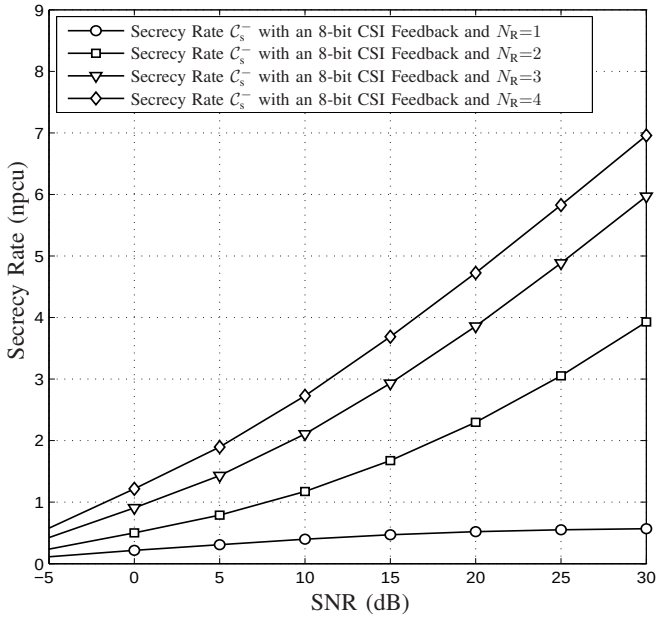

Fig. 6. Achievable secrecy rate with N_T=2, N_E=1, 8 bits feedback, and different values for the number of antennas at the legitimate receiver, N_R=1, 2, 3, 4.

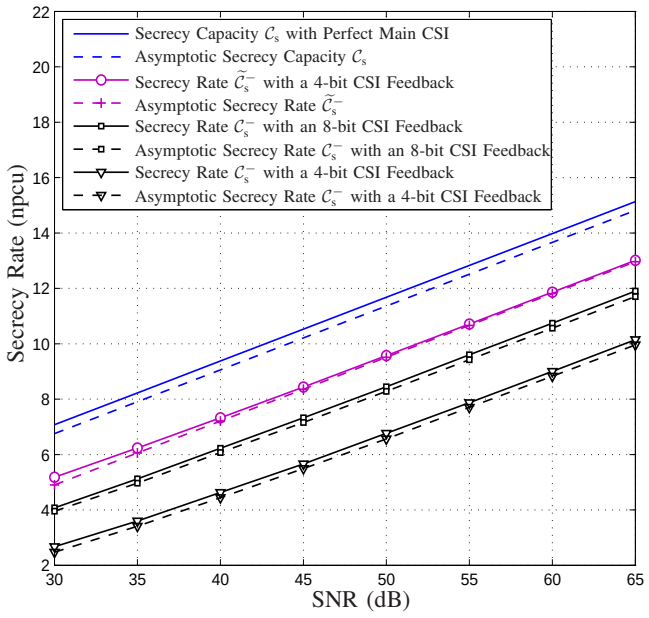

Fig. 8. Asymptotic secrecy rates for i.i.d. Rayleigh fading channels with N_T=N_R=2, N_E=1 and two values for the number of CSI feedback bites, B=4 and B=8.

as the eavesdropper, N_R=N_E=1 in this case, the achievable secrecy rate is very low compared to when the legitimate receiver has more antennas.

In Figure 7, the achievable secrecy rate $\mathcal{C}_s^-$ is presented along with the secrecy capacity $\mathcal{C}_s$ when 8 bits are used for CSI feedback, N_R=2, and N_E=1. The figure compares the cases when the transmitter has one antenna, N_T=1, two antennas, N_T=2, and four antennas, N_T=4. We can see that the secrecy throughput increases as the number of antennas at the transmitter augments. Also, we can see that the bounds are very tight when N_T=1 as the size of the main channel gain matrix is small compared to the other cases, i.e., $\mathbf{H}_R$ is a 2 by 1 matrix in this case. An 8-bit CSI feedback almost achieves the secrecy capacity with perfect main CSI when N_T=1, N_R=2, and N_E=1.

Figure 8 illustrates the asymptotic analysis, in the high SNR regime, when the transmitter and the legitimate receiver has two antennas, i.e., N_T=N_R=2, and the eavesdropper is equipped with one antenna, i.e., N_E=1. The respective asymptotic curves representing the achievable secrecy rate $\mathcal{C}_s^-$ and the secrecy capacity $\mathcal{C}_s$ approach, very tightly, the exact curves. Besides, the asymptotic curve of the achievable secrecy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

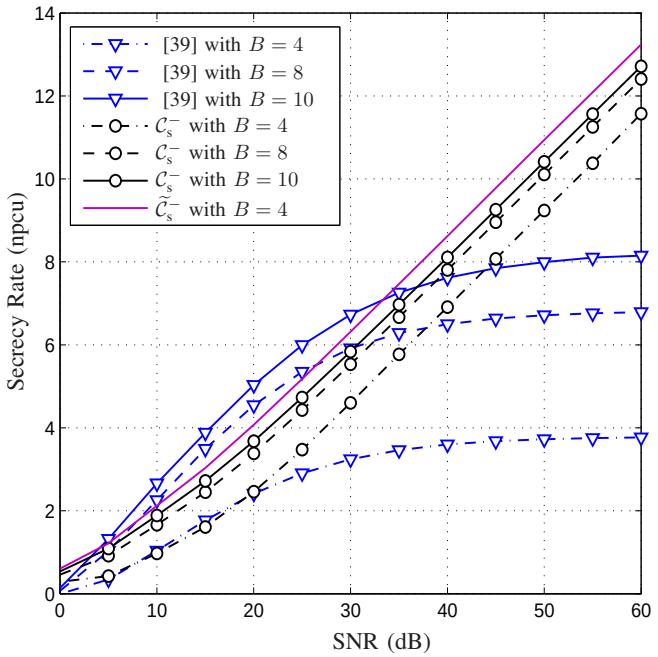

Fig. 9. Achievable secrecy rates $\mathcal{C}_s^-$, $\widetilde{\mathcal{C}}_s^-$, and $\hat{R}_M(\alpha)$ in [39], with N_T=4, N_R=2, N_E=1, and α=0.5.

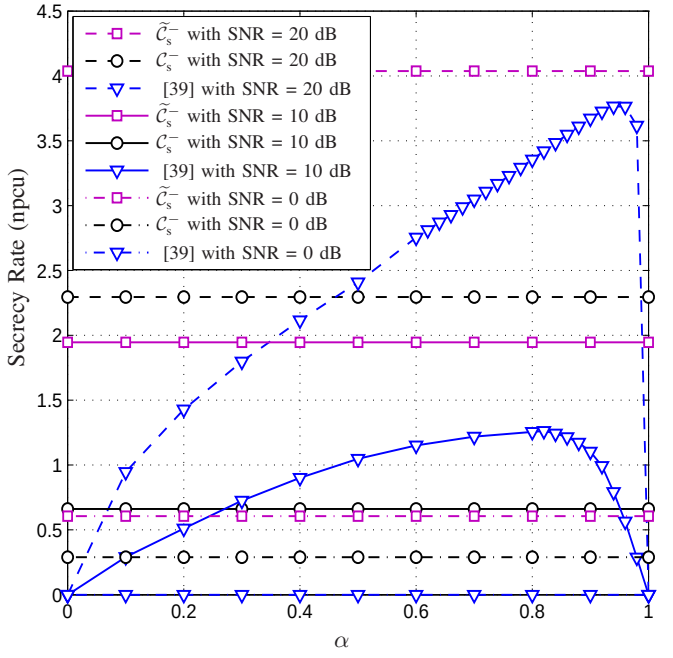

Fig. 10. Achievable secrecy rates $\mathcal{C}_s^-$, $\widetilde{\mathcal{C}}_s^-$, and $\hat{R}_M(\alpha)$ in [39], with N_T=4, N_R=2, N_E=1, and B=4.

rate $\widetilde{\mathcal{C}}_s^-$ coincides perfectly with the exact curve.

A comparison between our achievable secrecy rates $\mathcal{C}_s^-$ and $\widetilde{\mathcal{C}}_s^-$, and the achievable secrecy rate studied by [39], given by eq. (27) in the reference in question, is illustrated in Figures 9 and 10. In Figure 9, we present the achievable secrecy rates for three different values of the number of feedback bits, $B = 4, 8$, and 10, with $N_T = 4$, $N_R = 2$, $N_E = 1$, and $\alpha = 0.5$. The parameter α, in [39], represents the power splitting factor, i.e., $\alpha P_{avg}/N_R$ is used for data transmission and $(1-\alpha)P_{avg}/(N_T-N_R)$ is used for AN transmission. We can see that the transmission of AN is preferable for certain values of the SNR especially when the number of feedback bits is large. However, as we can see from Figure 9, for a fixed value of B, the achievable secrecy rate in [39] is bounded while $\mathcal{C}_s^-$ and $\widetilde{\mathcal{C}}_s^-$ are not. In Figure 10, we illustrate the achievable secrecy rates in terms of the factor α for three different values of the SNR, SNR=0 dB, 10 dB, and 20 dB, with $N_T = 4$, $N_R = 2$, $N_E = 1$, and $B = 4$. As no AN transmission is considered in our work, the secrecy rates remain constant. In the case when SNR=0 dB, we can that the achievable secrecy rate in [39] is equal to zero while $\mathcal{C}_s^-$ and $\widetilde{\mathcal{C}}_s^-$ are not. In the other two cases, we can see that the AN transmission is preferable compared to $\mathcal{C}_s^-$ only when the power allocated to the AN is restricted ($\alpha \gtrsim 0.5$).

VI. Conclusion

The impact of having limited main CSI feedback on the ergodic secrecy performance of a multiple-antenna block-fading wiretap channel has been investigated. We presented two achievable secrecy rates $\mathcal{C}_s^-$ and $\widetilde{\mathcal{C}}_s^-$ and an upper bound on the ergodic secrecy capacity $\mathcal{C}_s^+$, and showed that even with a 1-bit CSI feedback, a positive secrecy rate can still be achieved. The first achievable secrecy rate $\mathcal{C}_s^-$ adapts both the power and the transmission rate and guarantees that the best the eavesdropper can receive is the fixed transmission rate received at the legitimate node. The second achievable rate $\widetilde{\mathcal{C}}_s^-$ only adapt the power and is more convenient when the number of antennas at the eavesdropper is less than the number of antennas at the legitimate receiver, and the number of CSI feedback bits is small. Furthermore, we showed that the achievable secrecy rate $\mathcal{C}_s^-$ and the upper bound $\mathcal{C}_s^+$ coincide, asymptotically, as the capacity of the feedback link becomes large, i.e. $B \to \infty$; hence, fully characterizing the ergodic secrecy capacity in this case. Asymptotic analysis, in the high SNR regime, were also presented, and the gap between the bounds was estimated. In particular, we characterized the scaling behavior of the presented bounds, and showed that the asymptotic gap between $\mathcal{C}_s$ and $\mathcal{C}_s^-$ vanishes as the number of feedback bits increases while the asymptotic gap between $\mathcal{C}_s$ and $\widetilde{\mathcal{C}}_s^-$ is independent of the number of feedback bits.

In this paper, we assumed that the feedback bits are provided to the transmitter by the legitimate receiver through an error-free public link with limited capacity. An interesting future direction would be to investigate the secrecy performance of the system when the feedback link is subject to transmission errors. Another future direction would consist of considering the multi-antenna multi-users case.

Appendix A
Proof of Corollary 2

Considering uniform power allocation over all transmit antennas, at all times, and using the expression of the achievable secrecy rate in (3), we have

$$\mathcal{C}_s^{FF} \geq \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathbb{E}_{\mathbf{H}_E|\mathbf{H}_R\in\mathcal{H}_q} \left[\left\{ \log \frac{\min\limits_{\mathbf{H}_R\in\mathcal{H}_q} \left| \mathbf{I}_{N_R} + \frac{P_{avg}}{\sigma_R^2 N_T} \mathbf{H}_R \mathbf{H}_R^* \right|}{\left| \mathbf{I}_{N_E} + \frac{P_{avg}}{\sigma_E^2 N_T} \mathbf{H}_E \mathbf{H}_E^* \right|} \right\}^+ \right] P_q \tag{46}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

$$= \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathbb{E}_{\boldsymbol{\lambda}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\left\{ \min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}} \sum_{i=1}^{r_{\mathrm{R}}} \log\left(1+\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{R}_i}\right) - \sum_{i=1}^{r_{\mathrm{E}}} \log\left(1+\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{E}_i}\right) \right\}^{+} \right] P_q, \quad (47)$$

with $r_{\mathrm{R}}=\min(N_{\mathrm{T}},N_{\mathrm{R}})$, $r_{\mathrm{E}}=\min(N_{\mathrm{T}},N_{\mathrm{E}})$, and $\boldsymbol{\lambda}_{\mathrm{R}}$ and $\boldsymbol{\lambda}_{\mathrm{E}}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_{\mathrm{R}}\mathbf{H}_{\mathrm{R}}^*$ and $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^*$, i.e., $\boldsymbol{\lambda}_{\mathrm{R}}=\{\lambda_{\mathrm{R}_1},\cdots,\lambda_{\mathrm{R}_{r_{\mathrm{R}}}}\}$ and $\boldsymbol{\lambda}_{\mathrm{E}}=\{\lambda_{\mathrm{E}_1},\cdots,\lambda_{\mathrm{E}_{r_{\mathrm{E}}}}\}$. Taking $P_{\mathrm{avg}}\to\infty$, the terms $\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{R}_i}$ and $\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{E}_i}$, in (47), become dominant and we can write

$$\lim_{P_{\mathrm{avg}}\to\infty} \mathcal{C}_{\mathrm{s}}^{\mathrm{FF}}$$

$$\geq \lim_{P_{\mathrm{avg}}\to\infty} \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathbb{E}_{\boldsymbol{\lambda}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\left\{ \min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}} \sum_{i=1}^{r_{\mathrm{R}}} \log\left(\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{R}_i}\right) - \sum_{i=1}^{r_{\mathrm{E}}} \log\left(\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{E}_i}\right) \right\}^{+} \right] P_q \quad (48)$$

$$= \lim_{P_{\mathrm{avg}}\to\infty} \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathbb{E}_{\boldsymbol{\lambda}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\left\{ (r_{\mathrm{R}}-r_{\mathrm{E}}) \log\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} + \min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}} \sum_{i=1}^{r_{\mathrm{R}}} \log\frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{r_{\mathrm{E}}} \log\frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} \right\}^{+} \right] P_q. \quad (49)$$

We can, then, rewrite the limit in the following form

$$\lim_{P_{\mathrm{avg}}\to\infty} \left[\mathcal{C}_{\mathrm{s}}^{\mathrm{FF}} - \{r_{\mathrm{R}}-r_{\mathrm{E}}\}^{+} \log\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} \right] \geq \quad (50)$$

$$\lim_{P_{\mathrm{avg}}\to\infty} \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathbb{E}_{\boldsymbol{\lambda}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\left\{ (r_{\mathrm{R}}-r_{\mathrm{E}}) \log\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} + \min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}} \sum_{i=1}^{r_{\mathrm{R}}} \log\frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{r_{\mathrm{E}}} \log\frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} \right\}^{+} - \{r_{\mathrm{R}}-r_{\mathrm{E}}\}^{+} \log\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} \right] P_q.$$

In the special case when $r_{\mathrm{R}}=r_{\mathrm{E}}$, we get

$$\lim_{P_{\mathrm{avg}}\to\infty} \mathcal{C}_{\mathrm{s}}^{\mathrm{FF}} \geq \lim_{P_{\mathrm{avg}}\to\infty} \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathbb{E}_{\boldsymbol{\lambda}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\left\{ \min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}} \sum_{i=1}^{r_{\mathrm{R}}} \log\frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{r_{\mathrm{E}}} \log\frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} \right\}^{+} \right] P_q. \quad (51)$$

When $r_{\mathrm{R}} \neq r_{\mathrm{E}}$, we use the fact that the term $(r_{\mathrm{R}}-r_{\mathrm{E}})\log\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}}$ is dominant, and that

$$\{a+b\}^{+}-\{a\}^{+} = \begin{cases} b & \text{if } a>0 \\ 0 & \text{otherwise} \end{cases},$$

when a is dominant[2], to get

$$\lim_{P_{\mathrm{avg}}\to\infty} \left[\mathcal{C}_{\mathrm{s}}^{\mathrm{FF}} - \{r_{\mathrm{R}}-r_{\mathrm{E}}\}^{+} \log\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} \right] \geq$$

$$\begin{cases} \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathbb{E}_{\boldsymbol{\lambda}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}} \sum_{i=1}^{r_{\mathrm{R}}} \log\frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{r_{\mathrm{E}}} \log\frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} \right] P_q & \text{if } r_{\mathrm{R}}\geq r_{\mathrm{E}} \\ 0 & \text{if } r_{\mathrm{R}}<r_{\mathrm{E}} \end{cases},$$

This concludes our proof. □

APPENDIX B
PROOF OF COROLLARY 3

A. Lower Bounding the Secrecy Capacity with Perfect main CSI, $\mathcal{C}_s$, at High-SNR

We distinguish between two cases depending on the number of transmit antennas compared to the number of receive antennas.

- First Case: $N_{\mathrm{T}}\leq N_{\mathrm{R}}$

Using the expression of the ergodic secrecy capacity, in (6), and considering uniform power allocation over all transmit antennas, we can write

$$\lim_{P_{\mathrm{avg}}\to\infty} \mathcal{C}_{\mathrm{s}} \geq$$

$$\lim_{P_{\mathrm{avg}}\to\infty} \mathbb{E}_{\mathbf{H}_{\mathrm{E}},\mathbf{H}_{\mathrm{R}}} \left[\left\{ \log\frac{\left|\mathbf{I}_{N_{\mathrm{R}}}+\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}}\mathbf{H}_{\mathrm{R}}\mathbf{H}_{\mathrm{R}}^*\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}}+\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^*\right|} \right\}^{+} \right] \quad (52)$$

$$= \lim_{P_{\mathrm{avg}}\to\infty} \mathbb{E}_{\boldsymbol{\lambda}_{\mathrm{R}},\boldsymbol{\lambda}_{\mathrm{E}}} \left[\left\{ \sum_{i=1}^{N_{\mathrm{T}}} \log\left(1+\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{R}_i}\right) - \sum_{i=1}^{\min(N_{\mathrm{T}},N_{\mathrm{E}})} \log\left(1+\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{E}_i}\right) \right\}^{+} \right] \quad (53)$$

$$= \lim_{P_{\mathrm{avg}}\to\infty} \mathbb{E}_{\boldsymbol{\lambda}_{\mathrm{R}},\boldsymbol{\lambda}_{\mathrm{E}}} \left[\left\{ \sum_{i=1}^{N_{\mathrm{T}}} \log\left(\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{R}_i}\right) - \sum_{i=1}^{\min(N_{\mathrm{T}},N_{\mathrm{E}})} \log\left(\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{E}_i}\right) \right\}^{+} \right] \quad (54)$$

$$= \lim_{P_{\mathrm{avg}}\to\infty} \mathbb{E}_{\boldsymbol{\lambda}_{\mathrm{R}},\boldsymbol{\lambda}_{\mathrm{E}}} \left[\left\{ \{N_{\mathrm{T}}-N_{\mathrm{E}}\}^{+} \log\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} + \sum_{i=1}^{N_{\mathrm{T}}} \log\frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{\min(N_{\mathrm{T}},N_{\mathrm{E}})} \log\frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} \right\}^{+} \right], \quad (55)$$

where $\boldsymbol{\lambda}_{\mathrm{R}}$ and $\boldsymbol{\lambda}_{\mathrm{E}}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_{\mathrm{R}}\mathbf{H}_{\mathrm{R}}^*$ and $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^*$, i.e., $\boldsymbol{\lambda}_{\mathrm{R}}=\{\lambda_{\mathrm{R}_1},\cdots,\lambda_{\mathrm{R}_{r_{\mathrm{R}}}}\}$ and $\boldsymbol{\lambda}_{\mathrm{E}}=\{\lambda_{\mathrm{E}_1},\cdots,\lambda_{\mathrm{E}_{r_{\mathrm{E}}}}\}$. Then, using the fact that, when a is dominant, $\{a+b\}^{+}-\{a\}^{+} = \begin{cases} b & \text{if } a>0 \\ 0 & \text{otherwise} \end{cases}$, we get the following result

$$\lim_{P_{\mathrm{avg}}\to\infty} \left[\mathcal{C}_{\mathrm{s}} - \{N_{\mathrm{T}}-N_{\mathrm{E}}\}^{+} \log\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} \right] \geq$$

$$\begin{cases} 0 & \text{if } N_{\mathrm{T}}<N_{\mathrm{E}} \\ \mathbb{E}_{\boldsymbol{\lambda}_{\mathrm{R}},\boldsymbol{\lambda}_{\mathrm{E}}} \left[\sum_{i=1}^{N_{\mathrm{T}}} \log\frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{N_{\mathrm{E}}} \log\frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} \right] & \text{if } N_{\mathrm{E}}\leq N_{\mathrm{T}}\leq N_{\mathrm{R}} \end{cases}. \quad (56)$$

- Second Case: $N_{\mathrm{T}}>N_{\mathrm{R}}$

When the number of transmit antennas is larger than the number of receive antennas, i,e., $N_{\mathrm{T}}>N_{\mathrm{R}}$, we consider a uniform power transmitting scheme that broadcasts artificial noise over the null space of $\mathbf{H}_{\mathrm{R}}$. Let $\mathbf{H}_{\mathrm{R}} = \mathbf{U}_{\mathrm{R}}\boldsymbol{\lambda}_{\mathrm{R}}\mathbf{V}_{\mathrm{R}}^*$

[2] a is dominant in the sense that the sign of the sum $a+b$ is dictated by the sign of a.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

be the singular value decomposition (SVD) of $\mathbf{H}_{\mathrm{R}}$, where $\mathbf{U}_{\mathrm{R}} \in \mathbb{C}^{N_{\mathrm{R}} \times N_{\mathrm{R}}}$ and $\mathbf{V}_{\mathrm{R}} \in \mathbb{C}^{N_{\mathrm{T}} \times N_{\mathrm{T}}}$ are unitary matrices. Then, we can write matrix $\mathbf{V}_{\mathrm{R}}$ in the form $\mathbf{V}_{\mathrm{R}} = [\tilde{\mathbf{V}}_{\mathrm{R}}, \mathbf{Z}]$, with $\mathbf{Z} = \mathrm{null}(\mathbf{H}_{\mathrm{R}}) \in \mathbb{C}^{N_{\mathrm{T}} \times (N_{\mathrm{T}} - N_{\mathrm{R}})}$, such that $\mathbf{H}_{\mathrm{R}}\mathbf{Z} = 0_{N_{\mathrm{R}} \times (N_{\mathrm{T}} - N_{\mathrm{R}})}$ and the N_{R} columns of $\tilde{\mathbf{V}}_{\mathrm{R}} \in \mathbb{C}^{N_{\mathrm{T}} \times N_{\mathrm{R}}}$ span the orthogonal complement subspace to $\mathbf{Z}$. Since perfect CSI is assumed in this case, the transmitter has perfect knowledge of the precoding matrix $\mathbf{V}_{\mathrm{R}}$ and transmits $\mathbf{X} = \sqrt{P_{\mathrm{avg}}/N_{\mathrm{T}}}\left(\tilde{\mathbf{V}}_{\mathrm{R}}\mathbf{u} + \mathbf{Z}\mathbf{v}\right)$, where $\mathbf{u} \in \mathbb{C}^{N_{\mathrm{R}}}$ is the information vector and $\mathbf{v} \in \mathbb{C}^{N_{\mathrm{T}} - N_{\mathrm{R}}}$ is the artificial noise vector. Both $\mathbf{u}$ and $\mathbf{v}$ are assumed to be circular symmetric Gaussian random vectors with i.i.d. zero mean and unit variance entries. The respective received signals at the intended receiver and the eavesdropper can, then, be written as

$$\begin{aligned} \mathbf{Y}_{\mathrm{R}} &= \sqrt{\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}}}\mathbf{H}_{\mathrm{R}}\tilde{\mathbf{V}}_{\mathrm{R}}\mathbf{u} + \mathbf{Z}_{\mathrm{R}} \\ \mathbf{Y}_{\mathrm{E}} &= \sqrt{\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}}}\mathbf{H}_{\mathrm{E}}\tilde{\mathbf{V}}_{\mathrm{R}}\mathbf{u} + \sqrt{\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}}}\mathbf{H}_{\mathrm{E}}\mathbf{Z}\mathbf{v} + \mathbf{Z}_{\mathrm{E}}. \end{aligned} \tag{57}$$

Hence, the secrecy capacity can be characterized, in the high-SNR regime, as

$$\begin{aligned} \lim_{P_{\mathrm{avg}}\to\infty} \mathcal{C}_{\mathrm{s}} &\geq \lim_{P_{\mathrm{avg}}\to\infty} \mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}},\mathbf{H}_{\mathrm{R}}} \left[\left\{ \log \left| \mathbf{I}_{N_{\mathrm{R}}} + \frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}} \mathbf{H}_{\mathrm{R}}\mathbf{H}_{\mathrm{R}}^* \right| \right. \right. \\ &\left. \left. - \log \frac{\left| \mathbf{I}_{N_{\mathrm{E}}} + \frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}} \mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^* + \frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}} \mathbf{H}_{\mathrm{E}}\mathbf{Z}\mathbf{Z}^*\mathbf{H}_{\mathrm{E}}^* \right|}{\left| \mathbf{I}_{N_{\mathrm{E}}} + \frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}} \mathbf{H}_{\mathrm{E}}\mathbf{Z}\mathbf{Z}^*\mathbf{H}_{\mathrm{E}}^* \right|} \right\}^+ \right] \end{aligned} \tag{58}$$

$$\begin{aligned} &= \lim_{P_{\mathrm{avg}}\to\infty} \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{R}},\boldsymbol{\lambda}_{\mathrm{EZ}},\boldsymbol{\lambda}_{\mathrm{sum}}} \left[\left\{ \sum_{i=1}^{N_{\mathrm{R}}} \log \left(1 + \frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}} \lambda_{\mathrm{R}_i} \right) \right. \right. \\ &\left. \left. + \sum_{i=1}^{\min(N_{\mathrm{T}}-N_{\mathrm{R}},N_{\mathrm{E}})} \log \left(1 + \frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}} \lambda_{\mathrm{EZ}_i} \right) - \sum_{i=1}^{N_{\mathrm{E}}} \log \left(1 + \frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}} \lambda_{\mathrm{sum}_i} \right) \right\}^+ \right] \end{aligned} \tag{59}$$

$$\begin{aligned} &= \lim_{P_{\mathrm{avg}}\to\infty} \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{R}},\boldsymbol{\lambda}_{\mathrm{EZ}},\boldsymbol{\lambda}_{\mathrm{sum}}} \left[\left\{ \sum_{i=1}^{N_{\mathrm{R}}} \log \left(\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}} \lambda_{\mathrm{R}_i} \right) \right. \right. \\ &\left. \left. + \sum_{i=1}^{\min(N_{\mathrm{T}}-N_{\mathrm{R}},N_{\mathrm{E}})} \log \left(\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}} \lambda_{\mathrm{EZ}_i} \right) - \sum_{i=1}^{N_{\mathrm{E}}} \log \left(\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}} \lambda_{\mathrm{sum}_i} \right) \right\}^+ \right] \end{aligned} \tag{60}$$

$$\begin{aligned} &= \lim_{P_{\mathrm{avg}}\to\infty} \mathop{\mathbb{E}}_{\substack{\boldsymbol{\lambda}_{\mathrm{R}},\boldsymbol{\lambda}_{\mathrm{EZ}},\\ \boldsymbol{\lambda}_{\mathrm{sum}}}} \left[\left\{ \min\left(N_{\mathrm{T}} - N_{\mathrm{E}}, N_{\mathrm{R}}\right) \log \frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} \right. \right. \\ &\left. \left. + \sum_{i=1}^{N_{\mathrm{R}}} \log \frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} + \sum_{i=1}^{\min(N_{\mathrm{T}}-N_{\mathrm{R}},N_{\mathrm{E}})} \log \frac{\lambda_{\mathrm{EZ}_i}}{\sigma_{\mathrm{E}}^2} - \sum_{i=1}^{N_{\mathrm{E}}} \log \frac{\lambda_{\mathrm{sum}_i}}{\sigma_{\mathrm{E}}^2} \right\}^+ \right] \end{aligned} \tag{61}$$

where $\boldsymbol{\lambda}_{\mathrm{R}}$, $\boldsymbol{\lambda}_{\mathrm{E}}$, $\boldsymbol{\lambda}_{\mathrm{EZ}}$ and $\boldsymbol{\lambda}_{\mathrm{sum}}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_{\mathrm{R}}\mathbf{H}_{\mathrm{R}}^*$, $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^*$, $\mathbf{H}_{\mathrm{E}}\mathbf{Z}\mathbf{Z}^*\mathbf{H}_{\mathrm{E}}^*$ and $(\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^* + \mathbf{H}_{\mathrm{E}}\mathbf{Z}\mathbf{Z}^*\mathbf{H}_{\mathrm{E}}^*)$, i.e., $\boldsymbol{\lambda}_{\mathrm{R}} = \{\lambda_{\mathrm{R}_1}, \cdots, \lambda_{\mathrm{R}_{r_{\mathrm{R}}}}\}$, $\boldsymbol{\lambda}_{\mathrm{E}} = \{\lambda_{\mathrm{E}_1}, \cdots, \lambda_{\mathrm{E}_{r_{\mathrm{E}}}}\}$, $\boldsymbol{\lambda}_{\mathrm{EZ}} = \{\lambda_{\mathrm{EZ}_1}, \cdots, \lambda_{\mathrm{EZ}_{r_{\mathrm{EZ}}}}\}$ and $\boldsymbol{\lambda}_{\mathrm{sum}} = \{\lambda_{\mathrm{sum}_1}, \cdots, \lambda_{\mathrm{sum}_{r_{\mathrm{sum}}}}\}$. Once again, using the fact that, when a is dominant,

$$\{a+b\}^+ - \{a\}^+ = \begin{cases} b & \text{if } \ a > 0 \\ 0 & \text{otherwise} \end{cases},$$

we obtain

$$\begin{aligned} &\lim_{P_{\mathrm{avg}}\to\infty} \left[\mathcal{C}_{\mathrm{s}} - \min\left(\{N_{\mathrm{T}} - N_{\mathrm{E}}\}^+, N_{\mathrm{R}} \right) \log \frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} \right] \geq \\ &\begin{cases} \mathop{\mathbb{E}}_{\substack{\boldsymbol{\lambda}_{\mathrm{R}},\boldsymbol{\lambda}_{\mathrm{EZ}},\\ \boldsymbol{\lambda}_{\mathrm{sum}}}} \left[\sum_{i=1}^{N_{\mathrm{R}}} \log \frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} + \sum_{i=1}^{\min(N_{\mathrm{T}}-N_{\mathrm{R}},N_{\mathrm{E}})} \log \frac{\lambda_{\mathrm{EZ}_i}}{\sigma_{\mathrm{E}}^2} - \sum_{i=1}^{N_{\mathrm{E}}} \log \frac{\lambda_{\mathrm{sum}_i}}{\sigma_{\mathrm{E}}^2} \right] & \\ & \text{if } N_{\mathrm{T}} > \max(N_{\mathrm{E}}, N_{\mathrm{R}}) \\ 0 & \text{if } N_{\mathrm{T}} < N_{\mathrm{E}} \end{cases}. \end{aligned} \tag{62}$$

B. Upper Bounding the Secrecy Capacity with Perfect main CSI, $\mathcal{C}_s$, at High-SNR

Since the secrecy capacity when both the main and the eavesdropper's CSI are available at the transmitter upper bounds the secrecy capacity when only the main CSI is known at the transmitter, the upper bound results directly from [15, Theorem 2] and [16].

This concludes our proof. □

APPENDIX C
PROOF OF COROLLARY 4

Considering uniform power allocation over all transmit antennas, the constants θ_1 and θ_2 in Corollary 2 and Corollary 3, respectively, are equal to their respective lour bounding terms. Thus, the asymptotic difference between $\mathcal{C}_{\mathrm{s}}$ and $\mathcal{C}_{\mathrm{s}}^-$ can be characterized, when $N_{\mathrm{T}} \leq N_{\mathrm{R}}$, as

$$\begin{aligned} \lim_{P_{\mathrm{avg}}\to\infty} \left[\mathcal{C}_{\mathrm{s}} - \mathcal{C}_{\mathrm{s}}^- \right] &= \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{R}},\boldsymbol{\lambda}_{\mathrm{E}}} \left[\sum_{i=1}^{N_{\mathrm{T}}} \log \frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{N_{\mathrm{E}}} \log \frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} \right] \\ &- \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{E}}} \left[\min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q}} \sum_{i=1}^{N_{\mathrm{T}}} \log \frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{N_{\mathrm{E}}} \log \frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} \right] P_q \end{aligned} \tag{63}$$

$$\begin{aligned} &= \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{R}},\boldsymbol{\lambda}_{\mathrm{E}}} \left[\sum_{i=1}^{N_{\mathrm{T}}} \log \frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{N_{\mathrm{E}}} \log \frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} \right. \\ &\left. - \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q}} \sum_{i=1}^{N_{\mathrm{T}}} \log \frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{N_{\mathrm{E}}} \log \frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} P_q \right] \end{aligned} \tag{64}$$

$$= \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{R}}} \left[\sum_{i=1}^{N_{\mathrm{T}}} \log \lambda_{\mathrm{R}_i} - \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} P_q \min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q}} \sum_{i=1}^{N_{\mathrm{T}}} \log \lambda_{\mathrm{R}_i} \right] \tag{65}$$

where $\boldsymbol{\lambda}_{\mathrm{R}}$ and $\boldsymbol{\lambda}_{\mathrm{E}}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_{\mathrm{R}}\mathbf{H}_{\mathrm{R}}^*$ and $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^*$, i.e., $\boldsymbol{\lambda}_{\mathrm{R}} = \{\lambda_{\mathrm{R}_1}, \cdots, \lambda_{\mathrm{R}_{r_{\mathrm{R}}}}\}$ and $\boldsymbol{\lambda}_{\mathrm{E}} = \{\lambda_{\mathrm{E}_1}, \cdots, \lambda_{\mathrm{E}_{r_{\mathrm{E}}}}\}$.

The gap between $\mathcal{C}_{\mathrm{s}}$ and $\widetilde{\mathcal{C}}_{\mathrm{s}}^-$ can be deduced, directly, using $\{a\}^+ - a = \{-a\}^+$. □

REFERENCES

[1] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

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

[3] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[4] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

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

[6] I. Telatar, "Capacity of multi-antenna Gaussian channels," *European Transactions on Telecommunications*, vol. 10, pp. 585–595, Dec. 1999.

[7] L. Zheng and D. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels," *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.

[8] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. International Symposiumon on Information Theory (ISIT'2007)*, Nice, France, Jun. 2007, pp. 2471–2475.

[9] A. Khisti and G. Womell, "Secure transmission with multiple antennas Part I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[10] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annual Conference on Information Sciences and Systems (CISS'2007)*, Baltimore, MD, Mar. 2007, pp. 905 –910.

[11] S. Shafiee and S. Ulukus, "Achievable rates in gaussian MISO channels with secrecy constraints," in *Proc. International Symposiumon on Information Theory (ISIT'2007)*, Nice, France, Jun. 2007, pp. 2466–2470.

[12] E. Ekrem and S. Ulukus, "Secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[13] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

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

[15] A. Khisti and G. Womell, "Secure transmission with multiple antennas Part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[16] M. Yuksel and E. Erkip, "Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Transactions on Wireless Communications*, vol. 10, no. 3, pp. 762–771, Mar. 2011.

[17] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8812–8817, Oct. 2016.

[18] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the secrecy capacity of the wiretap channel under imperfect main channel estimation," *IEEE Transactions on Communications*, vol. 62, no. 10, pp. 3652–3664, Sep. 2014.

[19] A. Hyadi, Z. Rezki, A. Khisti, and M.-S. Alouini, "Secure broadcasting with imperfect channel state information at the transmitter," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2215–2230, Mar. 2016.

[20] Z. Chu, H. Xing, M. Johnston, and S. L. Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 283–297, Jan. 2016.

[21] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[22] N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," *IEEE Communications Letters*, vol. 17, no. 5, pp. 864–867, May 2013.

[23] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Transactions on Communications*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[24] J. Hu, Y. Cai, N. Yang, and W. Yang, "A new secure transmission scheme with outdated antenna selection," *IEEE Transactions on Forensics and Security*, vol. 10, no. 11, pp. 2435–2446, Nov. 2015.

[25] T.-Y. Liu, P.-H. Lin, Y.-W. P. Hong, and E. Jorswieck, "To avoid or not to avoid CSI leakage in physical layer secret communication systems," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 19–25, Dec. 2015.

[26] A. Hyadi, Z. Rezki, and M.-S. Alouini, "An overview of physical layer security in wireless communication systems with CSIT uncertainty," *IEEE Access*, vol. 4, pp. 6121–6132, Sep. 2016.

[27] R. W. Heath and A. Paulraj, "A simple scheme for transmit diversity using partial channel feedback," in *Proc. IEEE Asilomar Conference on in Signals, Systems and Computers*, Pacific Grove, CA, USA, Nov. 1998, pp. 1073–1078.

[28] R. S. Blum, "MIMO with limited feedback of channel state information," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '2003)*, Hong Kong, China, Apr. 2003, pp. 89–92.

[29] D. J. Love, R. W. Heath, and T. Strohmer, "Grassmannian beamforming for multiple-input multiple-output wireless systems," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2735–2747, Oct. 2003.

[30] V. Lau, Y. Liu, and T.-A. Chen, "On the design of MIMO blockfading channels with feedback-link capacity constraint," *IEEE Transactions on Communications*, vol. 52, no. 1, pp. 62–70, Jan. 2004.

[31] C. R. Murthy and B. D. Rao, "Quantization methods for equal gain transmission with finite rate feedback," *IEEE Transactions on Signal Processing*, vol. 55, no. 1, pp. 233–245, Jan. 2007.

[32] V. Lau, Y. Liu, and T.-A. Chen, "On the design of MIMO block-fading channels with feedback-link capacity constraint," *IEEE Transactions on Communications*, vol. 52, no. 1, pp. 62–70, Jan. 2004.

[33] D. Love, R. Heath, V. Lau, D. Gesbert, B. Rao, and M. Andrews, "An overview of limited feedback in wireless communication systems," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 8, pp. 1341–1365, Oct. 2008.

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

[35] A. Hyadi, Z. Rezki, and M.-S. Alouini, "On the secrecy capacity of the multiple-antenna wiretap channel with limited CSI feedback," in *Proc. IEEE Global Communications Conference (Globecom'2015)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[36] S. Liu, Y. Hong, and E. Viterbo, "Guaranteeing positive secrecy capacity for MIMOME wiretap channels with finite-rate feedback using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4193–4203, Aug. 2015.

[37] N. Li, X. Tao, and J. Xu, "Ergodic secrecy sum-rate for downlink multiuser MIMO systems with limited CSI feedback," *IEEE Communications Letters*, vol. 18, no. 6, pp. 969–972, Jun. 2014.

[38] X. Zhang, M. R. McKay, X. Zhou, and R. W. H. Jr, "Artificial-noise aided secure multi-antenna transmission with limited feedback," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2742–2754, May 2015.

[39] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y. P. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Transactions on Wireless Communications*, vol. 10, no. 3, pp. 901–915, Mar. 2011.

[40] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[41] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[42] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[43] S. Lloyd, "Least squares quantization in PCM," *IEEE Transactions on Information Theory*, vol. IT-28, no. 2, pp. 129–137, Mar. 1982.

[44] T. Yoo, N. Jindal, and A. Goldsmith, "Multi-antenna downlink channels with limited feedback and user selection," *IEEE Journal on Selected Areas of Communication*, vol. 25, no. 7, pp. 1478–1491, 2007.

[45] B. Hassibi and B. Hochwald, "How much training is needed in multiple-antenna wireless links," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 951–963, Apr. 2003.

[46] S. P. B. L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[47] G. Caire and S. Shamai, "On the capacity of some channels with channel state information," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 2007–2019, Sep. 1999.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2017.2727043, IEEE Transactions on Wireless Communications

Amal Hyadi (S'12) was born in Rabat, Morocco. She received the Diplôme d'Ingénieur from the Institut Nationale des Postes et Télécommunications (INPT), Rabat, Morocco, and the M.S. degree from King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia, in 2011 and 2013, respectively. She is currently pursuing the Ph.D. degree in electrical engineering at King Abdullah University of Science and Technology (KAUST). Her research interests include: physical layer security, performance analysis of cooperative cognitive systems and relay selection techniques.

Zouheir Rezki (S'01-M'08-SM'13) was born in Casablanca, Morocco. He received the Diplôme d'Ingénieur degree from the École Nationale de l'Industrie Minérale (ENIM), Rabat, Morocco, in 1994, the M.Eng. degree from École de Technologie Supérieure, Montreal, Québec, Canada, in 2003, and the Ph.D. degree from École Polytechnique, Montreal, Québec, in 2008, all in electrical engineering. From October 2008 to September 2009, he was a postdoctoral research fellow with Data Communications Group, Department of Electrical and Computer Engineering, University of British Columbia. Then, has been a Senior Research Scientist at King Abdullah University of Science and Technology (KAUST), Saudi Arabia until June 2016. He joined University of Idaho as a Faculty Member on August 2016. His research interests include: performance limits of communication systems, physical-layer security, cognitive and sensor networks and low-complexity detection algorithms.

Mohamed-Slim Alouini (S'94-M'98-SM'03-F'09) was born in Tunis, Tunisia. He received the Ph.D. degree in Electrical Engineering from the California Institute of Technology (Caltech), Pasadena, CA, USA, in 1998. He served as a faculty member in the University of Minnesota, Minneapolis, MN, USA, then in the Texas A&M University at Qatar, Education City, Doha, Qatar before joining King Abdullah University of Science and Technology (KAUST), Thuwal, Makkah Province, Saudi Arabia as a Professor of Electrical Engineering in 2009. His current research interests include the modeling, design, and performance analysis of wireless communication systems.