On the Secrecy Capacity of the Multiple-Antenna Wiretap Channel with Limited CSI Feedback

Amal Hyadi, Zouheir Rezki, and Mohamed-Slim Alouini
Computer, Electrical, and Mathematical Sciences & Engineering (CEMSE) Division
King Abdullah University of Science and Technology (KAUST), Thuwal, Makkah Province, Saudi Arabia
$\{$ amal.hyadi, zouheir.rezki, slim.alouini $\}$ @kaust.edu.sa

***Abstract*—We study the ergodic secrecy capacity of a block-fading wiretap channel when there are multiple antennas at the transmitter, the legitimate receiver and the eavesdropper. We consider that the receivers are aware of their respective channel matrices while the transmitter is only provided by a B-bits 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. Assuming an average transmit power constraint, we provide an upper and a 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 secrecy capacity in this case.**

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, and the new research directions towards the next wave of innovation known as the Internet of Things, 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 is known as Wireless Physical Layer Security. In his seminal work [1], Wyner introduced the degraded wiretap channel where a source exploits the structure of the medium channel to transmit a message reliably to the intended receiver, while leaking asymptotically no information to the eavesdropper. Ulterior works generalized Wyner's work to the case of non-degraded channels [2], Gaussian channels [3], and fading channels [4].

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 performance [5]. The problem of analyzing the secrecy capacity of multiple antenna systems has been of great interest in last years. The secrecy capacity for the multiple-input single-output (MISO) wiretap Gaussian channel has been proven in [6]–[8]. In [6], the authors furthermore give an upper bound for the MIMO case with asymptotic signal to noise ratio (SNR). Another work [9] characterizes 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 MIMO Gaussian channels has been investigated in [10], while the case of MIMO transmission with a multiple-antenna eavesdropper has been considered in [11]–[13] when the channel matrices are fixed and known.

Transmit beamforming is one of the simplest approaches to achieve full diversity in MIMO wireless systems. Unfortunately, to obtain the optimal performance, this method requires a complete knowledge of the channel state information (CSI) at the transmitter (CSIT) or the knowledge of the optimal beamforming vector; which are both difficult to have in practical scenarios. One way to overcome this challenge is by using feedback [14]. For the case of a single antenna transmission, an upper and a lower bounds on the secrecy capacity of the wiretap channel with finite rate feedback have been proposed in [15] for block-fading channels. For the MIMO case, the work in [16] analyzes a secrecy sum-rate for the downlink multiuser MIMO system, over fast fading channel, with limited CSI feedback. Another work [17] evaluates the impact of quantized channel direction information on the achievable secrecy rate, for multiple-antenna wiretap channels, using artificial noise and assuming that the channel of the eavesdropper is unknown at the transmitter.

In this paper, we investigate the secrecy capacity of multiple-antenna block-fading wiretap channels with limited CSI feedback. Indeed, we consider that the transmitter is unaware of the channel matrices of the main and the eavesdropper channels, and is only provided by a finite CSI feedback sent by the legitimate receiver through an error free link with limited capacity. Assuming an average power constraint at the transmitter, we provide an upper and a lower bounds on the ergodic secrecy capacity. Then, we present an optimal framework for feedback and transmission that maximizes the forward secrecy rate. For the particular case of infinite feedback, we prove that our bounds coincide; hence, fully characterizing the secrecy capacity in this case.

This work was supported by the Qatar National Research Fund (a member of Qatar Foundation) under NPRP Grant NPRP 5-603-2-243. The statements made herein are solely the responsibility of the authors.

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 while the optimal framework for feedback and transmission is provided in subsection III-B. Details on the analysis of the secrecy capacity bounds are presented in Section IV. Finally, selected numerical results are presented 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 $\mathbb{E}[.]$, $\log$ represents the natural logarithm unless otherwise indicated, and we define $\{\nu\}^{+}{=}\max(0,\nu)$. The entropy of a discrete random variable X is denoted by $H(X)$, and the mutual information between random variables X and Y is denoted by $I(X,Y)$. A sequence of length n is denoted by X^n, $X(k)$ represents the k-th element of X, and $X(l,k)$ the k-th element of X 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 $X \succeq 0$ indicates that X is positive semidefinite, and we use 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

$$\begin{aligned} Y_{\text{R}}(t) &= H_{\text{R}}(t)X(t) + Z_{\text{R}}(t) \\ Y_{\text{E}}(t) &= H_{\text{E}}(t)X(t) + Z_{\text{E}}(t) \end{aligned} \quad , \tag{1}$$

where $X(t)$ is the transmitted signal, $H_{\text{R}}(t) \in \mathbb{C}^{N_{\text{R}}\times N_{\text{T}}}$ and $H_{\text{E}}(t) \in \mathbb{C}^{N_{\text{E}}\times N_{\text{T}}}$ are the complex channel gain matrices, and $Z_{\text{R}}(t)$ and $Z_{\text{E}}(t)$ are, each, independent and identically distributed (i.i.d.) additive complex Gaussian noise vectors with zero mean and identity covariance matrix. We consider a block-fading channel where the channel gain matrices remain constant within a fading block of length $\kappa{>>}1$, i.e., $H_{\text{R}}(\kappa l) = H_{\text{R}}(\kappa l-1) = \cdots = H_{\text{R}}(\kappa l-\kappa+1) = H_{\text{R}}(l)$ and $H_{\text{E}}(\kappa l) = H_{\text{E}}(\kappa l{-}1) = \cdots = H_{\text{E}}(\kappa l{-}\kappa{+}1) = H_{\text{E}}(l)$, where $l = 1,\cdots,L$, and L is the total number of fading blocks. We assume that the channel encoding and decoding frames span a large number of fading blocks, i.e., L is large, and that the blocks change independently from a fading block to another. The channel input $\{X(t)\}_t$ is subject to an average total power constraint

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

where $n{=}\kappa L$.

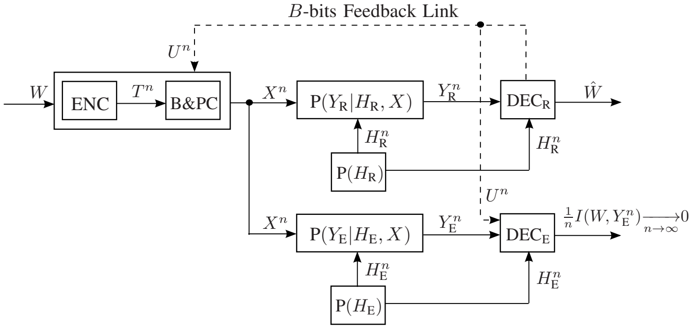

Fig. 1. Block diagram of the channel model.

We assume perfect CSI at the receiver sides. That is, the legitimate receiver is instantaneously aware of its channel gain matrix $H_{\text{R}}(l)$, and the eavesdropper knows $H_{\text{E}}(l)$, 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-bits 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. The message W must be kept confidential from the eavesdropper. Therefore, we impose a secrecy constraint on the information leakage-rate, $\frac{1}{n}I(W,Y_{\text{E}}^n)$, which is required to asymptotically approach zero as $n\to\infty$.

In the light of the work in [18], 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 H_{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.

At the transmitter side, each feedbacked information u_q corresponds to a unitary beamforming matrix V_q and a diagonal power control matrix Λ_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 T. The forward signal X can then be written in the form

$$X = V_q\Lambda_q^{1/2}T,$$

and we let $\mathbb{E}[T^*T]{=}1$ for normalization. By taking $\rho_q{=}V_q\Lambda_qV_q^*$, the respective received SNRs at the legitimate receiver and the eavesdropper are $H_{\text{R}}\rho_qH_{\text{R}}^*$ and $H_{\text{E}}\rho_qH_{\text{E}}^*$. Note that the chosen set of beamforming and power control matrices should satisfy the average power constraint, i.e., tr$\,[\mathbb{E}[\rho_q]]\,{\leq}P_{\text{avg}}$ for all $q\in\{1,\cdots,Q\}$, with the expectation taken over all channel gain realizations. It is assumed that all nodes are aware of the codebooks used for feedback and transmission. More details on the optimal codebooks generation are available on the following section.

III. Main Results

In this section, we present the main results obtained for the ergodic secrecy capacity of the considered system model. Also, 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-bits CSI feedback link, sent at the beginning of each fading block, and the average power constraint in (2), the following secrecy rate is achievable

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

where $Q{=}2^{B}$, $\mathrm{tr}\left[\mathbb{E}[\rho_q]\right]\leq P_{\mathrm{avg}}$, $\rho_q{\succeq}0$, and $P_q{=}\mathrm{Pr}\left[H_{\mathrm{R}}\in\mathcal{H}_q\right]$ 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 scheme.

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 $\mathcal{H}_q$, $q\in\{1,\cdots,Q\}$, the transmitter conveys codewords at rate $R_q=\min\limits_{H_{\mathrm{R}}\in\mathcal{H}_q}\log\left|I_{N_{\mathrm{R}}}+H_{\mathrm{R}}\rho_q H_{\mathrm{R}}^{*}\right|$, with the transmission strategy ρ_q. Rate R_q changes only periodically and is held constant over the duration interval of a fading block. Let T_q be a channel gain matrix from $\mathcal{H}_q$ satisfying $T_q=\arg\min\limits_{H_{\mathrm{R}}\in\mathcal{H}_q}\left|I_{N_{\mathrm{R}}}+H_{\mathrm{R}}\rho_q H_{\mathrm{R}}^{*}\right|$. 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 $\log\left|I_{N_{\mathrm{E}}}+H_{\mathrm{E}}\rho_q H_{\mathrm{E}}^{*}\right|$. We can then optimize over the main channel gain regions, $\mathcal{H}_q$'s, and the transmission strategies, ρ_q's, to maximize the secrecy rate.

Intuitively, Theorem 1 states that even a 1-bit feedback at the beginning of each fading block ensures a positive secrecy rate. We now present an upper bound on the 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-bits CSI feedback link, sent at the beginning of each fading block, and the average power constraint in (2), an upper bound on the secrecy capacity is given by

$$\mathcal{C}_{\mathrm{s}}^{+}=\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q,\rho_q\}}\mathop{\mathbb{E}}_{\substack{H_{\mathrm{R}}\in\mathcal{H}_q\\ H_{\mathrm{E}}}}\left[\left\{\log\frac{\left|I_{N_{\mathrm{R}}}+H_{\mathrm{R}}\rho_q H_{\mathrm{R}}^{*}\right|}{\left|I_{N_{\mathrm{E}}}+H_{\mathrm{E}}\rho_q H_{\mathrm{E}}^{*}\right|}\right\}^{+}\right]P_q, \tag{4}$$

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

Proof: The proof is provided in the following section.

Letting Q goes to ∞, the lower bound in (3) and the upper bound in (4) coincide, hence, fully characterizing the secrecy capacity in this case.

Corollary 1: The 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

$$\mathcal{C}_{\mathrm{s}}=\max_{\rho(H_{\mathrm{R}})}\mathop{\mathbb{E}}_{H_{\mathrm{E}},H_{\mathrm{R}}}\left[\left\{\log\frac{\left|I_{N_{\mathrm{R}}}+H_{\mathrm{R}}\rho(H_{\mathrm{R}})H_{\mathrm{R}}^{*}\right|}{\left|I_{N_{\mathrm{E}}}+H_{\mathrm{E}}\rho(H_{\mathrm{R}})H_{\mathrm{E}}^{*}\right|}\right\}^{+}\right], \tag{5}$$

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

Proof: Corollary 1 results directly from the expressions of the achievable rate in (3) and the upper bound in (4), by letting $P_q=\dfrac{1}{Q}$ and taking into consideration that as $Q\rightarrow\infty$, the set of partition regions, $\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$, becomes infinite and the legitimate receiver is basically forwarding matrix H_{R} to the transmitter. ■

To the best of our knowledge, this result has not been reported in earlier works. For the special case of $N_{\mathrm{T}}{=}N_{\mathrm{R}}{=}N_{\mathrm{E}}{=}1$, the secrecy capacity in corollary 1 coincides with the result in theorem 2 from reference [4].

B. Optimal Framework for Feedback and Transmission

Finding the optimal feedback strategy, $\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$, and the optimal transmission strategy, $\{\rho_1,\cdots,\rho_Q\}$, that maximizes the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$ in (3), 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

$$\delta\left(H_{\mathrm{R}},H_{\mathrm{E}},\rho_q\right)=-\left[\left\{\log\frac{\left|I_{N_{\mathrm{R}}}{+}H_{\mathrm{R}}\rho_q H_{\mathrm{R}}^{*}\right|}{\left|I_{N_{\mathrm{E}}}{+}H_{\mathrm{E}}\rho_q H_{\mathrm{E}}^{*}\right|}\right\}^{+}-\lambda\left(\mathrm{tr}\rho_q-P_{\mathrm{avg}}\right)\right], \tag{6}$$

where $\rho_q\succeq 0$ and $q=\{1,\cdots,Q\}$. We need to find the optimal $\{\mathcal{H}_1,\cdots,\mathcal{H}_Q\}$ and $\{\rho_1,\cdots,\rho_Q\}$ that minimizes the average distortion measure Δ given by

$$\Delta=\sum_{q=1}^{Q}\mathop{\mathbb{E}}_{H_{\mathrm{E}}}\left[\delta\left(T_q,H_{\mathrm{E}},\rho_q\right)\right]P_q, \tag{7}$$

where $T_q=\arg\min\limits_{H_{\mathrm{R}}\in\mathcal{H}_q}\left|I_{N_{\mathrm{R}}}{+}H_{\mathrm{R}}\rho_q H_{\mathrm{R}}^{*}\right|$, and $P_q=\mathrm{Pr}\left[H_{\mathrm{R}}{\in}\mathcal{H}_q\right]$.

To solve this optimization problem, we use Lloyd's algorithm [19]. The Optimal Framework for Feedback and Transmission (OFFT) for the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$ is given in Algo.1[1]. Note that Algo.1 is an offline optimization algorithm, and hence, complexity has a relatively small impact on implementation.

[1] In general, there is no guarantee that Lloyd's algorithm will converge to the global optimum [19].

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

```
Input  : $Q$, $P_{\text{avg}}$.
Output: Optimal feedback and transmission codebooks
        $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$ and $\{\rho_1, \cdots, \rho_Q\}$.
Consider a random partition of the space of $H_{\text{R}}$:
        $\mathbb{H}_1 = \{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$;
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
        $T_q(\rho_q) = \arg\min_{H_{\text{R}} \in \mathcal{H}_q} |I_{N_{\text{R}}} + H_{\text{R}}\rho_q H_{\text{R}}^*|$;
        Find the optimal transmission strategy:
            $\rho_q = \arg\min_{\rho_q} \mathbb{E}_{H_{\text{E}}} [\delta(T_q(\rho_q), H_{\text{E}}, \rho_q)] P_q$;
    for $q = 1 : Q$ do
        Find the optimal partition region:
        $\mathcal{H}_q = \{H_{\text{R}} : \delta(H_{\text{R}}, H_{\text{E}}, \rho_q) \leq \delta(H_{\text{R}}, H_{\text{E}}, \rho_j)$ ;
                $\forall j \in \{1, \cdots, Q\}, j \neq q\}$ ;
    $itr = itr + 1$;
    $\mathbb{H}_{itr} = \{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$;
```

IV. Ergodic Capacity Analysis

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

A. Proof of Achievability in Theorem 1

Given a partition of the channel gain space $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$ and a transmission strategy $\{\rho_1, \cdots, \rho_Q\}$, let T_q, $q \in \{1, \cdots, Q\}$, be the element of $\mathcal{H}_q$ that minimizes the function

$$\xi(H_{\text{R}}) = |I_{N_{\text{R}}} + H_{\text{R}}\rho_q H_{\text{R}}^*| ,$$

i.e., $\left|I_{N_{\text{R}}} + T_q\rho_q T_q^*\right| \leq |I_{N_{\text{R}}} + H_{\text{R}}\rho_q H_{\text{R}}^*|$, for all $H_{\text{R}} \in \mathcal{H}_q$.

We note that such a minimum exists since the function $\xi(H_{\text{R}})$ is concave, and $\mathcal{H}_q$ corresponds to a Voronoi region which is by definition a convex set. We assume that the rates

$$R_q = \log\left|I_{N_{\text{R}}} + T_q\rho_q T_q^*\right| , q \in \{1, \cdots, Q\},$$

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

$$R_{\text{s}}^{-} = \sum_{q=1}^{Q} P_q \mathop{\mathbb{E}}_{H_{\text{E}}} \left[\{R_q - \log|I_{N_{\text{E}}} + H_{\text{E}}\rho_q H_{\text{E}}^*|\}^+ \right] - \epsilon_1, \quad (8)$$

with $P_q = \Pr[H_{\text{R}} \in \mathcal{H}_q]$, is achievable. Let

$$R_{\text{e}} = \sum_{q=1}^{Q} P_q \mathop{\mathbb{E}}_{H_{\text{E}}} [\log|I_{N_{\text{E}}} + H_{\text{E}}\rho_q H_{\text{E}}^*|] - \epsilon_2. \quad (9)$$

The considered wiretap codebook is generated by uniformly partitioning random Gaussian codewords into $2^{nR_{\text{s}}^{-}}$ bins; each containing $2^{nR_{\text{e}}}$ codewords. 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 $R_q \leq \log|I_{N_{\text{R}}} + H_{\text{R}}\rho_q H_{\text{R}}^*|$ 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 $R_{\text{e}} \geq R_{\text{s}}^{-} - \epsilon$. We have

$$\begin{aligned} nR_{\text{e}} &= H(W|Y_{\text{E}}^n, H_{\text{E}}^L, U^L) &(10)\\ &\geq I(W; X^n|Y_{\text{E}}^n, H_{\text{E}}^L, U^L) &(11)\\ &= H(X^n|Y_{\text{E}}^n, H_{\text{E}}^L, U^L) - H(X^n|Y_{\text{E}}^n, H_{\text{E}}^L, U^L, W). &(12) \end{aligned}$$

On one hand, we can write

$$\begin{aligned} &H(X^n|Y_{\text{E}}^n, H_{\text{E}}^L, U^L)\\ &= \sum_{l=1}^{L} H(X^\kappa(l)|Y_{\text{E}}^\kappa(l), H_{\text{E}}(l), U(l)) &(13)\\ &\geq \sum_{l \in \mathcal{S}_L} H(X^\kappa(l)|Y_{\text{E}}^\kappa(l), H_{\text{E}}(l), U(l)) &(14)\\ &\geq \sum_{l \in \mathcal{S}_L} \kappa \left(\sum_{q=1}^{Q} P_q \left(R_q - \log|I_{N_{\text{E}}} + H_{\text{E}}(l)\rho_q H_{\text{E}}^*(l)|\right) - \epsilon' \right) &(15)\\ &= \sum_{l=1}^{L} \kappa \left(\sum_{q=1}^{Q} P_q \left\{R_q - \log|I_{N_{\text{E}}} + H_{\text{E}}(l)\rho_q H_{\text{E}}^*(l)|\right\}^+ - \epsilon' \right) &(16)\\ &= n \sum_{q=1}^{Q} P_q \mathop{\mathbb{E}}_{H_{\text{E}}} \left[\{R_q - \log|I_{N_{\text{E}}} + H_{\text{E}}\rho_q H_{\text{E}}^*|\}^+ \right] - n\epsilon' &(17)\\ &= nR_{\text{s}}^{-} - n\epsilon', &(18) \end{aligned}$$

where (13) results from the memoryless property of the channel and the independence of the $X^\kappa(l)$'s, (14) is obtained by removing all the terms corresponding to the fading blocks $l \notin \mathcal{S}_L$, with $\mathcal{S}_L = \{l \in \{1, \cdots, L\} : T_q(l) > H_{\text{E}}(l)\}$, and (17) 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], $\frac{1}{n} H(X^n|Y_{\text{E}}^n, H_{\text{E}}^L, U^L, W)$ vanishes as $n \to \infty$ and we can write

$$H(X^n|Y_{\text{E}}^n, H_{\text{E}}^L, U^L, W) \leq n\epsilon". \quad (19)$$

Substituting (18) and (19) in (12), we get $R_{\text{e}} \geq R_{\text{s}}^{-} - \epsilon$, with $\epsilon = \epsilon' + \epsilon"$, and ϵ' and $\epsilon"$ are selected to be arbitrarily small. Maximizing over the main channel gain partition regions $\mathcal{H}_q$ and the associated transmission strategies ρ_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

$$\begin{aligned}
nR_{\mathrm{E}} &= H(W|Y_{\mathrm{E}}^n, H_{\mathrm{E}}^L, U^L) \qquad (20)\\
&= H(W|Y_{\mathrm{E}}^n, H_{\mathrm{E}}^L, H_{\mathrm{R}}^L, U^L) \qquad (21)\\
&= I(W;Y_{\mathrm{R}}^n|Y_{\mathrm{E}}^n,H_{\mathrm{E}}^L,H_{\mathrm{R}}^L,U^L)+H(W|Y_{\mathrm{R}}^n,Y_{\mathrm{E}}^n,H_{\mathrm{E}}^L,H_{\mathrm{R}}^L,U^L) \qquad (22)\\
&\leq I(W;Y_{\mathrm{R}}^n|Y_{\mathrm{E}}^n, H_{\mathrm{E}}^L, H_{\mathrm{R}}^L, U^L)+n\epsilon \qquad (23)\\
&= \sum_{l=1}^{L}\sum_{k=1}^{\kappa} H(Y_{\mathrm{R}}(l,k)|Y_{\mathrm{E}}^n, H_{\mathrm{E}}^L, H_{\mathrm{R}}^L, U^L, Y_{\mathrm{R}}^{\kappa(l-1)+(k-1)})\\
&\quad - H(Y_{\mathrm{R}}(l,k)|W, Y_{\mathrm{E}}^n, H_{\mathrm{E}}^L, H_{\mathrm{R}}^L, U^L, Y_{\mathrm{R}}^{\kappa(l-1)+(k-1)})+n\epsilon \qquad (24)\\
&\leq \sum_{l=1}^{L}\sum_{k=1}^{\kappa} H(Y_{\mathrm{R}}(l,k)|Y_{\mathrm{E}}(l,k), H_{\mathrm{E}}(l), H_{\mathrm{R}}(l), U^l)\\
&\quad - H(Y_{\mathrm{R}}(l,k)|W,X(l,k),Y_{\mathrm{E}}^n, H_{\mathrm{E}}^L,H_{\mathrm{R}}^L,U^L,Y_{\mathrm{R}}^{\kappa(l-1)+(k-1)})+n\epsilon \qquad (25)\\
&= \sum_{l=1}^{L}\sum_{k=1}^{\kappa} H(Y_{\mathrm{R}}(l,k)|Y_{\mathrm{E}}(l,k), H_{\mathrm{E}}(l), H_{\mathrm{R}}(l), U^l)\\
&\quad - H(Y_{\mathrm{R}}(l,k)|X(l,k), Y_{\mathrm{E}}(l,k), H_{\mathrm{E}}(l), H_{\mathrm{R}}(l), U^l)+n\epsilon \qquad (26)\\
&= \sum_{l=1}^{L}\sum_{k=1}^{\kappa} I(X(l,k);Y_{\mathrm{R}}(l,k)|Y_{\mathrm{E}}(l,k),H_{\mathrm{E}}(l),H_{\mathrm{R}}(l),U^l)+n\epsilon \qquad (27)\\
&\leq \sum_{l=1}^{L}\sum_{k=1}^{\kappa} \left\{I(X(l,k);Y_{\mathrm{R}}(l,k)|H_{\mathrm{R}}(l),U^l)\right.\\
&\qquad\qquad \left. - I(X(l,k);Y_{\mathrm{E}}(l,k)|H_{\mathrm{E}}(l),U^l)\right\}^+ +n\epsilon \qquad (28)\\
&= \sum_{l=1}^{L}\kappa\left\{I(X(l);Y_{\mathrm{R}}(l)|H_{\mathrm{R}}(l),U^l)\right.\\
&\qquad\qquad \left. - I(X(l);Y_{\mathrm{E}}(l)|H_{\mathrm{E}}(l),U^l)\right\}^+ +n\epsilon, \qquad (29)
\end{aligned}$$

where (21) comes from the independence of W and H_{R}^L given Y_{E}^n, H_{E}^L and U^L, inequality (23) follows from the fact that

$$H(W|Y_{\mathrm{R}}^n, Y_{\mathrm{E}}^n, H_{\mathrm{E}}^L, H_{\mathrm{R}}^L, U^L){\leq}H(W|Y_{\mathrm{R}}^n, H_{\mathrm{R}}^L, U^L),$$

and Fano's inequality $H(W|Y_{\mathrm{R}}^n, H_{\mathrm{R}}^L, U^L){\leq}n\epsilon$, and (28) holds true following similar lines as [11]–[13]; since given $H_{\mathrm{R}}(l)$ and $H_{\mathrm{E}}(l)$, the channel at hand is a multiple antenna wiretap channel.

The right-hand side of (29) is maximized by a Gaussian input. That is, taking $X(l) \sim \mathcal{CN}\left(0, \omega_l^{1/2}(U^l)\right)$, with the power policy $\omega_l(U^l)$ satisfying the average power constraint, we can write

$$nR_{\mathrm{E}} \leq \sum_{l=1}^{L}\kappa \underset{\substack{U^l,H_{\mathrm{R}}(l)\\ H_{\mathrm{E}}(l),}}{\mathbb{E}}\left[\left\{\log\frac{|I_{N_{\mathrm{R}}}{+}H_{\mathrm{R}}(l)\omega_l(U^l)H_{\mathrm{R}}^*(l)|}{|I_{N_{\mathrm{E}}}{+}H_{\mathrm{E}}(l)\omega_l(U^l)H_{\mathrm{E}}^*(l)|}\right\}^+\right]{+}n\epsilon \tag{30}$$

$$\leq \sum_{l=1}^{L}\kappa \underset{\substack{U(l),\\ H_{\mathrm{R}}(l),\\ H_{\mathrm{E}}(l)}}{\mathbb{E}}\left[\left\{\log\frac{|I_{N_{\mathrm{R}}}{+}H_{\mathrm{R}}(l)\underset{U^{l-1}}{\mathbb{E}}[\omega_l(U^l)|U(l)]\,H_{\mathrm{R}}^*(l)|}{|I_{N_{\mathrm{E}}}{+}H_{\mathrm{E}}(l)\underset{U^{l-1}}{\mathbb{E}}[\omega_l(U^l)|U(l)]\,H_{\mathrm{E}}^*(l)|}\right\}^+\right]{+}n\epsilon \tag{31}$$

$$= \sum_{l=1}^{L}\kappa \underset{\substack{U(l),\\ H_{\mathrm{R}}(l),\\ H_{\mathrm{E}}(l)}}{\mathbb{E}}\left[\left\{\log\frac{|I_{N_{\mathrm{R}}}{+}H_{\mathrm{R}}(l)\Omega_l(U(l))H_{\mathrm{R}}^*(l)|}{|I_{N_{\mathrm{E}}}{+}H_{\mathrm{E}}(l)\Omega_l(U(l))H_{\mathrm{E}}^*(l)|}\right\}^+\right] + n\epsilon \tag{32}$$

$$= \sum_{l=1}^{L}\kappa \underset{U,H_{\mathrm{R}},H_{\mathrm{E}}}{\mathbb{E}}\left[\left\{\log\frac{|I_{N_{\mathrm{R}}}{+}H_{\mathrm{R}}\Omega_l(U)H_{\mathrm{R}}^*|}{|I_{N_{\mathrm{E}}}{+}H_{\mathrm{E}}\Omega_l(U)H_{\mathrm{E}}^*|}\right\}^+\right] + n\epsilon, \tag{33}$$

where (31) is obtained by using Jensen's inequality since the function $X \to \left\{\log\frac{|I{+}AXA^*|}{|I{+}BXB^*|}\right\}^+$ is concave over the set of nonnegative definite matrices, $\Omega_l(U(l))$ in (32) is defined as $\Omega_l(U(l)){=}\underset{U^{l-1}}{\mathbb{E}}\left[\omega_l(U^l)|U(l)\right]$, and where (33) follows from the ergodicity and the stationarity of the channel gains, i.e., the expectation in (32) does not depend on the block fading index. Thus, we have

$$R_{\mathrm{E}} \leq \frac{1}{L}\sum_{l=1}^{L} \underset{U,H_{\mathrm{R}},H_{\mathrm{E}}}{\mathbb{E}}\left[\left\{\log\frac{|I_{N_{\mathrm{R}}}{+}H_{\mathrm{R}}\Omega_l(U)H_{\mathrm{R}}^*|}{|I_{N_{\mathrm{E}}}{+}H_{\mathrm{E}}\Omega_l(U)H_{\mathrm{E}}^*|}\right\}^+\right] + \epsilon \tag{34}$$

$$\leq \underset{U,H_{\mathrm{R}},H_{\mathrm{E}}}{\mathbb{E}}\left[\left\{\log\frac{\left|I_{N_{\mathrm{R}}}{+}H_{\mathrm{R}}\dfrac{1}{L}\displaystyle\sum_{l=1}^{L}\Omega_l(U)H_{\mathrm{R}}^*\right|}{\left|I_{N_{\mathrm{E}}}{+}H_{\mathrm{E}}\dfrac{1}{L}\displaystyle\sum_{l=1}^{L}\Omega_l(U)H_{\mathrm{E}}^*\right|}\right\}^+\right] + \epsilon \tag{35}$$

$$= \underset{U,H_{\mathrm{R}},H_{\mathrm{E}}}{\mathbb{E}}\left[\left\{\log\frac{|I_{N_{\mathrm{R}}}{+}H_{\mathrm{R}}\Omega(U)H_{\mathrm{R}}^*|}{|I_{N_{\mathrm{E}}}{+}H_{\mathrm{E}}\Omega(U)H_{\mathrm{E}}^*|}\right\}^+\right] + \epsilon, \tag{36}$$

where (35) comes from applying Jensen's inequality once again, and where $\Omega(U)$ in (36) 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 ρ_q, for each $q \in \{1, \cdots, Q\}$, concludes the proof. ■

V. Numerical Results

In this section, we provide selected simulation results for the case of i.i.d. Rayleigh fading channels. Figure 2 illustrates the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^-$, in nats per channel use (npcu), when the transmitter, the legitimate receiver and the eavesdropper have 2 antennas, i.e. $N_{\mathrm{T}}{=}N_{\mathrm{R}}{=}N_{\mathrm{E}}{=}2$. The secrecy capacity $\mathcal{C}_{\mathrm{s}}$, from Corollary 1, is also presented in Fig. 2 as a benchmark. It represents the secrecy capacity with full main CSI at the transmitter. We can see that, as the capacity of the feedback link grows, i.e., the number of bits B increases, the achievable rate grows toward the secrecy capacity $\mathcal{C}_{\mathrm{s}}$.

In Figure 3, the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^-$ is presented along with the secrecy capacity $\mathcal{C}_{\mathrm{s}}$ when both the transmitter

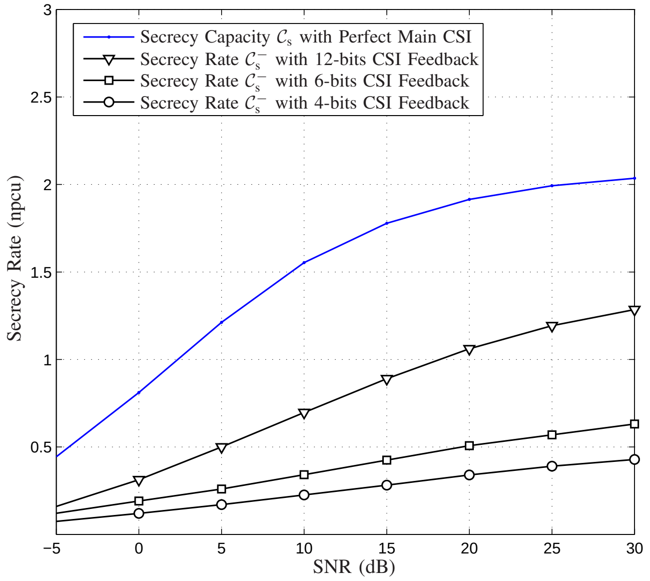

Fig. 2. Achievable secrecy rate, for Rayleigh fading channels, with N_{T}=N_{R}=N_{E}=2 and various B-bits feedback, B=4, 6, 12.

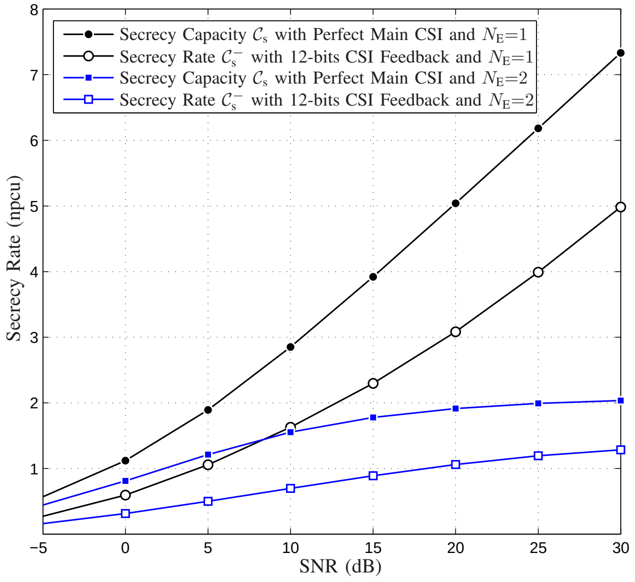

Fig. 3. Comparison of the achievable secrecy rates when the eavesdropper has one and two antennas with N_{T}=N_{R}=2 and 12-bits feedback.

and the legitimate receiver have two antennas, i.e. N_{T}=N_{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_{E}=1 and when he has two, i.e. N_{E}=2. As expected, the secrecy rate is higher when the eavesdropper has fewer antennas compared to the transmitter and the legitimate receiver.

VI. Conclusion

In this paper, we investigated the secrecy capacity of the multiple-antenna block-fading wiretap channel with limited CSI feedback. Assuming full CSI on the receivers' side and an average power constraint at the transmitter, we presented an achievable secrecy rate and an upper bound on the ergodic secrecy capacity when the feedback link is limited to B bits per fading block. In order to maximize the secrecy rate, we presented a framework that generates the optimal feedback and transmission codebooks. Furthermore, we showed 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 secrecy capacity in this case.

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

[6] 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.

[7] 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.

[8] 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.

[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] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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