Secure DoF of MIMO Rayleigh Block Fading Wiretap Channels with No CSI Anywhere

Ta-Yuan Liu[1], Pritam Mukherjee[2], Sennur Ulukus[2], Shih-Chun Lin[3], and Y.-W. Peter Hong[1]

[1]Inst. of Communication Eng. & Dept. of Electrical Eng., National Tsing Hua University, Hsinchu, Taiwan 30013
[2]Dept. of Electrical and Computer Eng., University of Maryland, College Park, MD 20742
[3]Dept. of Electronic and Computer Eng., National Taiwan University of Science and Technology, Taipei, Taiwan 10607

***Abstract*—We consider the block Rayleigh fading multiple-input multiple-output (MIMO) wiretap channel with no prior channel state information (CSI) available at any of the terminals. The channel gains remain constant in a coherence time of T symbols, and then change to another independent realization. The transmitter, the legitimate receiver and the eavesdropper have n_t, n_r and n_e antennas, respectively. We determine the exact secure degrees of freedom (s.d.o.f.) of this system when $T \geq 2\min(n_t, n_r)$. We show that, in this case, the s.d.o.f. is exactly $(\min(n_t, n_r) - n_e)^+(T - \min(n_t, n_r))/T$. The first term can be interpreted as the eavesdropper with n_e antennas taking away n_e antennas from both the transmitter and the legitimate receiver. The second term can be interpreted as a fraction of s.d.o.f. being lost due to the lack of CSI at the legitimate receiver. In particular, the fraction loss, $\min(n_t, n_r)/T$, can be interpreted as the fraction of channel uses dedicated to training the legitimate receiver for it to learn its own CSI. We prove that this s.d.o.f. can be achieved by employing a constant norm channel input, which can be viewed as a generalization of discrete signalling to multiple dimensions.**

I. Introduction

We consider the wiretap channel where a legitimate transmitter wishes to have information-theoretically secure communication with a legitimate receiver in the presence of an eavesdropper. The wiretap channel was introduced by Shannon [1] for the case of noiseless channels, where it was shown that secure keys and one-time-pad encryption was necessary for secure communications. The noisy wiretap channel was introduced by Wyner, who determined the capacity-equivocation region for the degraded case [2]. Csiszar and Korner generalized his result to arbitrary, not necessarily degraded, wiretap channels [3]. Leung-Yan-Cheong and Hellman determined the capacity-equivocation region of the Gaussian wiretap channel and showed that Gaussian signaling is optimal [4]. The s.d.o.f. of the scalar Gaussian wiretap channel is zero.

The MIMO wiretap channel where the legitimate entities and the eavesdropper have multiple antennas was considered for the 2-2-1 case in [5] and the general case in [6]–[8]. These references determined the exact secrecy capacity of the MIMO wiretap channel for the case of full CSI at all terminals, and showed that no channel prefixing is necessary and Gaussian signalling is optimal. It can be deduced from these works that the s.d.o.f. of the MIMO wiretap channel with full CSI is $\min((n_t - n_e)^+, n_r)$, where $(x)^+ = \max(x, 0)$.

The fading wiretap channel with a single antenna at all terminals, where all parties have perfect CSI of all links was considered in [9]–[12]. Modeling the fading wiretap under full CSI as a bank of independent parallel channels, these references showed that independent Gaussian signalling in all parallel channels, together with water-filling of the total power over these channels, is optimal. Reference [13] considered the single antenna wiretap channel where the transmitter has the legitimate receiver's CSI but no eavesdropper CSI under the assumption of infinite coherence times for channel fading, and showed that Gaussian signalling is optimal in this case. Reference [14] considered the same model under a fast fading condition (single symbol coherence time), and showed that M-QAM signaling or Gaussian signaling with added Gaussian artificial noise, may outperform plain Gaussian signalling. In the single antenna fading channel, under all CSI conditions, the s.d.o.f. is zero, since it is zero under perfect CSI.

Using multiple antennas at the legitimate users however, non-zero s.d.o.f. may be achieved even under partial CSI conditions. Reference [15] showed that in MIMO wiretap channel with perfect CSI at the receivers, but only a statistical CSI at the transmitter, under a fast fading Rayleigh channel, the s.d.o.f. of the system is $(\min(n_t, n_r) - n_e)^+$. Note that this may be less than the s.d.o.f. achievable under perfect CSI, which is $\min((n_t - n_e)^+, n_r)$. A comparison of these two s.d.o.f. may be interpreted as the eavesdropper taking away n_e antennas only from the transmitter in the case of perfect CSI [5]–[8], but n_e antennas from both the transmitter and the legitimate receiver in the case of partial CSI [15]. More strongly, reference [16] considered the case of an arbitrarily varying eavesdropper in a MIMO wiretap channel and showed that the same s.d.o.f. of $(\min(n_t, n_r) - n_e)^+$ can be achieved in this case. In [16], the CSI of the legitimate receiver is assumed known at the transmitter, however, nothing is known about the eavesdropper CSI, not even its probability distribution. This is an exceptionally strong modeling of the eavesdropper, where secrecy must be guaranteed for every realization of the eavesdropper channel; in a way, the eavesdropper may be thought to be controlling its channel adversarially.

All above work considered that some (either perfect or partial) CSI is available at some of the terminals. In practice, typically, the way CSI becomes available at the terminals is via the receivers measuring it and feeding it back to the transmitters. It is reasonable to assume that no CSI is known

at the outset before the start of the communication. One must then take into consideration the cost of acquiring the CSI. In addition, the assumption of perfect CSI is an idealization; in reality, the terminals can only have an estimate of the channel in a delayed manner. Further, in most cases, eavesdropper CSI will not be available at the transmitter, because she will not feed her measurement back, and even if she does, she will not be truthful. Thus, it is more practical to assume that no CSI is available at any terminal a priori. Recently, reference [17] studied the case where no CSI is available at any terminal and the coherence time of the Rayleigh fading channel is one symbol duration. Reference [17] determined the exact secrecy capacity in this case and showed that discrete signalling is optimal. As in all other single antenna cases, the s.d.o.f. in [17] is zero. It can be shown that, even when multiple antennas are added, s.d.o.f. in the case of fast fading in [17] is still zero.

In this paper, we consider the MIMO wiretap channel under block Rayleigh fading, where the channel gains of both the legitimate receiver and the eavesdropper remain fixed for T symbols, and then change to another independent realization. This models a Rayleigh fading wireless communication channel with a coherence time of T symbol durations. We consider the case when neither the transmitter nor the receivers have any CSI. This can be considered as an extension of [17] to the case of multiple antennas and larger (than one) coherence times. A similar channel model without any secrecy constraints was considered in [18], [19], where in [18] the structure of the optimal input distribution was found, and in [19] the d.o.f. was determined to be $m(1-m/T)$ where $m=\min(n_t,n_r,\lfloor T/2\rfloor)$. Our work can also be considered as a wiretap version of [18], [19].

We show that when the coherence time T satisfies $T \geq 2\min(n_t,n_r)$, the s.d.o.f. of this system is exactly $(\min(n_t,n_r)-n_e)^+(T-\min(n_t,n_r))/T$. Compared to the MIMO wiretap channel results in [15], [16], where the legitimate receiver knows its channel gain, the s.d.o.f. in our case is exactly the same as those in [15], [16] except for a factor of $(T-\min(n_t,n_r))/T$. Intuitively, at high signal-to-noise ratio (SNR), the legitimate receiver needs $\min(n_t,n_r)$ channel uses out of T channel uses to learn its channel. Therefore, the factor $(T-\min(n_t,n_r))/T$ intuitively accounts for the number of channel uses lost for estimating the channel at the legitimate receiver. As in the cases of [15], [16], due to no CSI at the transmitter, the eavesdropper takes away n_e antennas from both the transmitter and the receiver, i.e., n_e is subtracted from $\min(n_t,n_r)$, as opposed to being subtracted only from n_t as in the case of full CSI at the transmitter [5]–[8]. In comparison to the case without any secrecy constraints in [18], [19], here we have a subtraction of n_e from the first term in the d.o.f. due to the presence of the eavesdropper.

Finally, it is interesting to note that one cannot achieve a positive s.d.o.f with either a long coherence time in a single antenna system [13] or with multiple antennas in a very short ($T=1$) coherence time channel [17]; however, with some moderate coherence ($T\geq 2\min(n_t,n_r)$) and use of multiple antennas, it is possible to achieve positive s.d.o.f.

II. System Model and Problem Formulation

Consider a wiretap channel that consists of a transmitter with n_t antennas, a legitimate receiver with n_r antennas, and an eavesdropper with n_e antennas. The channel between the transmitter and the legitimate receiver is denoted by $\mathbf{H}\in\mathcal{C}^{n_r\times n_t}$ and the channel between the transmitter and the eavesdropper is denoted by $\mathbf{G}\in\mathcal{C}^{n_e\times n_t}$. The channels are Rayleigh fading with entries of $\mathbf{H}$ and $\mathbf{G}$ being i.i.d. complex Gaussian random variables with zero-mean and unit-variance, i.e., $\mathcal{CN}(0,1)$. The unit-variance assumption is without loss of generality as the difference in the channel qualities may be modeled by different noise variances at the two receivers. The channels are block fading, i.e., the channel coefficients remain constant in a coherence interval T and change independently across different intervals according to the same distribution.

Let $\mathbf{X}\in\mathcal{C}^{n_t\times T}$ denote the signal transmitted by the transmitter during a coherence interval. The transmitted signal is subject to an average power constraint as,

$$\frac{1}{T}\mathbb{E}\left[\mathrm{tr}(\mathbf{X}\mathbf{X}^\dagger)\right]\leq P \tag{1}$$

where $\mathrm{tr}(\cdot)$ denotes the trace function. The received signal at the legitimate receiver and the eavesdropper are

$$\mathbf{Y}=\mathbf{H}\mathbf{X}+\mathbf{N}_r \tag{2}$$

$$\mathbf{Z}=\mathbf{G}\mathbf{X}+\mathbf{N}_e \tag{3}$$

where $\mathbf{N}_r\in\mathcal{C}^{n_r\times T}$ and $\mathbf{N}_e\in\mathcal{C}^{n_e\times T}$ are additive white Gaussian noises with i.i.d. entries with distributions $\mathcal{CN}(0,\sigma_r^2)$ and $\mathcal{CN}(0,\sigma_e^2)$, respectively. The CSI, i.e., the realizations of $\mathbf{H}$ and $\mathbf{G}$, are not known to any of the terminals.

A $(2^{nR},n)$ code consists of an encoder f_n at the transmitter that maps each secret message, say $W\in\mathcal{W}\triangleq\{1,\ldots,2^{nR}\}$ into a length-n codeword and a decoder g_n at the legitimate receiver that maps its received signal into a message estimate $\hat{W}\in\mathcal{W}$. Each codeword is transmitted over multiple coherence intervals [18] and n is chosen as a multiple of T. The signal received at the legitimate receiver and the eavesdropper over n channel uses are denoted by $\mathbf{Y}^n$ and $\mathbf{Z}^n$, respectively.

A secret rate R is said to be achievable if there exists an encoder f_n and a decoder g_n such that the probability of error at the legitimate receiver $\mathbb{P}(W\neq\hat{W})$ goes to zero and the average equivocation at the eavesdropper measured by $\frac{1}{n}H(W|\mathbf{Z}^n)$ approaches $\frac{1}{n}H(W)$, as the codeword length $n\to\infty$. The secrecy capacity C_s is the supremum of all such achievable secrecy rates. From [3], the secrecy capacity is

$$C_s=\frac{1}{T}\max_{V,\mathbf{X}}\ I(V;\mathbf{Y})-I(V;\mathbf{Z}) \tag{4}$$

where V is an auxiliary random variable that satisfies the Markov chain $V\to\mathbf{X}\to\mathbf{Y},\mathbf{Z}$. Determining the optimal joint distribution of $(V,\mathbf{X})$ and the resulting exact secrecy capacity expression is challenging, instead, in this paper, we focus on determining the s.d.o.f. which is defined as,

$$D_s=\lim_{P\to\infty}\frac{C_s}{\log P} \tag{5}$$

III. Summary of the Main Results

In this section, we summarize our main results. We provide the proofs in the following sections. The main results of our paper can be encapsulated through the following three lemmas which leads to the conclusion in Theorem 1.

Lemma 1 *For the MIMO wiretap channel in* (2)-(3)*, with no CSI at any terminal,*

$$D_s = 0, \quad \text{if } n_r \leq n_e \tag{6}$$

This implies that the secrecy capacity does not scale with power when the eavesdropper has more antennas than the legitimate user. We can however achieve positive s.d.o.f. when $n_r > n_e$ as stated in the following two lemmas.

Lemma 2 *When $n_t \geq n_r > n_e$, and $T \geq 2n_r$, the s.d.o.f. is given by*

$$D_s = (n_r - n_e)\left(\frac{T - n_r}{T}\right) \tag{7}$$

Lemma 3 *When $n_r > n_e$, $n_r > n_t$, and $T \geq 2n_t$, the s.d.o.f. is given by*

$$D_s = (n_t - n_e)^+\left(\frac{T - n_t}{T}\right) \tag{8}$$

We combine the above three lemmas and have the following theorem as the main result of our paper.

Theorem 1 *For the MIMO wiretap channel in* (2)-(3)*, with no CSI at any terminal, when $T \geq 2\min(n_t, n_r)$, the s.d.o.f. is given by*

$$D_s = (\min(n_t, n_r) - n_e)^+\left(\frac{T - \min(n_t, n_r)}{T}\right) \tag{9}$$

Notice that the s.d.o.f. is affected by two factors. The factor $(\min(n_t, n_r) - n_e)^+$ in Theorem 1 comes from the difference between the d.o.f. of the main channel and that of the eavesdropper's channel, and the factor $(1 - \min(n_t, n_r)/T)$ is due to the lack of knowledge of the CSI. One can regard the ratio $\min(n_t, n_r)/T$ as the cost of channel estimation from the point of view of a training based scheme.

IV. Proof of Lemma 1

To prove Lemma 1, we will in fact prove the following stronger result for this case:

$$C_s \leq \left[n_e \log\left(1 + \frac{P}{\sigma_r^2}\right) - n_e \log\left(1 + \frac{P}{\sigma_e^2}\right)\right]^+ \tag{10}$$

In order to derive this upper bound on the secrecy capacity, since $n_r \leq n_e$ in this case, we first notice that for a fixed n_e, the secrecy capacity of the MIMO wiretap channel with $n_r = n_e$ is always greater than or equal to that of the case with $n_r < n_e$. Hence it suffices to upper bound the secrecy capacity of the system with $n_r = n_e$, which we will call the *enhanced wiretap channel*.

For the enhanced wiretap channel, if $\sigma_r^2 \geq \sigma_e^2$, it is clear that the legitimate user is stochastically degraded with respect to the eavesdropper. Hence, the secrecy capacity in this case is zero. However, if $\sigma_r^2 < \sigma_e^2$, using the two conditions $n_r = n_e$ and $\sigma_r^2 < \sigma_e^2$, we can construct a degraded wiretap channel equivalent to (2)-(3) as follows

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{N}_r \tag{11}$$

$$\mathbf{Z}' = \mathbf{H}\mathbf{X} + \mathbf{N}_r + \mathbf{N}_e' = \mathbf{Y} + \mathbf{N}_e' \tag{12}$$

where each element of $\mathbf{N}_e' \in \mathcal{C}^{n_e \times T}$ is i.i.d. Gaussian with zero-mean and variance $\sigma_e^2 - \sigma_r^2$, and $\mathbf{N}_e'$ is independent of $\mathbf{X}$, $\mathbf{H}$, and $\mathbf{N}_r$. The equivalent channel in (11)-(12) has the same secrecy capacity as the original one in (2)-(3), since the secrecy capacity depends only on the conditional marginal probabilities $p(\mathbf{Y}|\mathbf{X})$ and $p(\mathbf{Z}|\mathbf{X})$. For the equivalent model in (11)-(12), we have $\mathbf{X} \to \mathbf{Y} \to \mathbf{Z}'$. Thus, from [2], [3], no channel prefixing is required and the secrecy capacity of the equivalent degraded wiretap channel (11)-(12) is given by

$$C_s = \frac{1}{T} \max_{p_{\mathbf{X}} \in S_{p_{\mathbf{X}}}} I(\mathbf{X}; \mathbf{Y}) - I(\mathbf{X}; \mathbf{Z}') \tag{13}$$

where $S_{p_{\mathbf{X}}}$ denotes the set of all input distributions which satisfy the power constraint in (1).

To derive the upper bound in (10), we first rewrite (13) as

$$T \cdot C_s = \max_{p_{\mathbf{X}} \in S_{p_{\mathbf{X}}}} h(\mathbf{Y}) - h(\mathbf{Z}') - h(\mathbf{Y}|\mathbf{X}) + h(\mathbf{Z}'|\mathbf{X}) \tag{14}$$

Now we introduce the following lemma which is a vector generalization of [17, eqn. (12)].

Lemma 4 *If $n_r = n_e$ and $\sigma_r^2 < \sigma_e^2$, we have the following inequality for the wiretap channel in* (11)-(12)

$$h(\mathbf{Y}|\mathbf{X}) - h(\mathbf{Z}'|\mathbf{X}) \geq h(\mathbf{Y}|\mathbf{X}, \mathbf{H}) - h(\mathbf{Z}'|\mathbf{X}, \mathbf{H}) \tag{15}$$

Using Lemma 4 in (14), we obtain

$$\begin{aligned} T \cdot C_s &\leq \max_{p_{\mathbf{X}} \in S_{p_{\mathbf{X}}}} h(\mathbf{Y}) - h(\mathbf{Y} + \mathbf{N}_e') \\ &\qquad - h(\mathbf{Y}|\mathbf{X}, \mathbf{H}) + h(\mathbf{Z}'|\mathbf{X}, \mathbf{H}) \qquad (16) \\ &\leq n_e \log\left(1 + \frac{P}{\sigma_r^2}\right) - n_e \log\left(1 + \frac{P}{\sigma_e^2}\right) \qquad (17) \end{aligned}$$

where we used the entropy power inequality and the fact that Gaussian maximizes differential entropy, noting that $\mathbb{E}[\mathrm{tr}(\mathbf{Y}\mathbf{Y}^\dagger)] \leq (P + \sigma_r^2) n_e T$. This gives us the desired result in (10), completing the proof of Lemma 1.

V. Proof of Lemma 2

Due to space limitations, we outline the steps of the proof and skip some of the details. We first prove the converse and then provide a scheme that achieves the desired s.d.o.f.

A. Converse

To find an upper bound for the s.d.o.f. D_s, we only need to consider the case where $\sigma_r^2 < \sigma_e^2$, since with all other channel parameters remaining the same, the wiretap channel (2)-(3) with $\sigma_r^2 < \sigma_e^2$ yields larger secrecy capacity than that with

$\sigma_r^2 \geq \sigma_e^2$. Under the assumption $\sigma_r^2 < \sigma_e^2$, we can once again construct a degraded equivalent channel (as we did in (11)-(12) for $n_r = n_e$), without changing C_s by selecting n_e row vectors from n_r rows of the legitimate channel matrix $\mathbf{H}$ to form the eavesdropper's channel. For any fixed partition $\mathrm{p}_1 \cup \mathrm{p}_2 = \{1, \ldots, n_r\}$ where $|\mathrm{p}_1| = n_e$ and $\mathrm{p}_2 = \{1, \ldots, n_r\} \setminus \mathrm{p}_1$, we construct a degraded equivalent channel for (2)-(3) as follows

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{N}_r \tag{18}$$

$$\mathbf{Z}^{\mathrm{p}_1} = \mathbf{H}^{\mathrm{p}_1}\mathbf{X} + \mathbf{N}_r^{\mathrm{p}_1} + \mathbf{N}_e' = \mathbf{Y}^{\mathrm{p}_1} + \mathbf{N}_e' \tag{19}$$

where $\mathbf{H}^{\mathrm{p}_1}, \mathbf{N}_e^{\mathrm{p}_1}$ and $\mathbf{Y}^{\mathrm{p}_1}$ denote the collection of row vectors with indices belonging to p_1 from $\mathbf{H}, \mathbf{N}_e$ and $\mathbf{Y}$, respectively. $\mathbf{Z}^{\mathrm{p}_1}$ denotes the equivalent eavesdropper's received signal constructed from $\mathbf{Y}^{\mathrm{p}_1}$. For any partition $(\mathrm{p}_1, \mathrm{p}_2)$, as in the proof of Lemma 1, the secrecy capacity of the degraded wiretap channel (18)-(19) is

$$C_s = \frac{1}{T} \max_{p_{\mathbf{X}} \in S_{p_{\mathbf{X}}}} I(\mathbf{X}; \mathbf{Y}) - I(\mathbf{X}; \mathbf{Z}^{\mathrm{p}_1}) \tag{20}$$

First, we characterize the optimal input structure for the equivalent degraded channel given in (18)-(19). This helps us restrict possible input distributions and simplify the problem. Interestingly, due to the degradedness of the equivalent wiretap channel in (18)-(19) and the concavity of the secrecy capacity in the input distribution for degraded channels [17], the optimal input structure in (20) is the same as that in the channel without secrecy constraints in [18].

Recall that a random matrix $\mathbf{M} \in \mathcal{C}^{N \times T}$ where $T \geq N$ is *isotropically distributed* (i.d.) if the following equation holds

$$p(\mathbf{M}) = p(\mathbf{M}\mathbf{U}) \tag{21}$$

for all deterministic $T \times T$ unitary matrices $\mathbf{U}$. The optimal input structure for the equivalent degraded wiretap channel in (18)-(19) is characterized in the following lemma.

Lemma 5 *When $n_r > n_e$ and $\sigma_r^2 < \sigma_e^2$, for the equivalent channel in* (18)-(19)*, the optimal input distribution that maximizes C_s in* (20) *has the structure*

$$\mathbf{X} = \mathbf{\Lambda}\mathbf{\Theta} \tag{22}$$

if $T \geq n_t$, where $\mathbf{\Lambda}$ is an $n_t \times T$ diagonal random matrix with real and non-negative diagonal elements, and $\mathbf{\Theta}$ is a $T \times T$ i.d. unitary matrix which is independent of $\mathbf{\Lambda}$.

Although we cannot completely characterize the optimal $\mathbf{X}$, the results in Lemma 5 suffice to derive a useful upper bound for D_s. We can rewrite the secrecy capacity given in (20) and upper bound it as

$$T \cdot C_s = \max_{p_{\mathbf{X}} \in S^*_{p_{\mathbf{X}}}} I(\mathbf{X}; \mathbf{Y}) - I(\mathbf{X}; \mathbf{Z}^{\mathrm{p}_1}) \tag{23}$$

$$= \max_{p_{\mathbf{X}} \in S^*_{p_{\mathbf{X}}}} h(\mathbf{Y}^{\mathrm{p}_1}) + h(\mathbf{Y}^{\mathrm{p}_2}|\mathbf{Y}^{\mathrm{p}_1}) - h(\mathbf{Y}^{\mathrm{p}_1} + \mathbf{N}_e') - h(\mathbf{Y}|\mathbf{X}) + h(\mathbf{Z}^{\mathrm{p}_1}|\mathbf{X}) \tag{24}$$

$$\leq \max_{p_{\mathbf{X}} \in S^*_{p_{\mathbf{X}}}} h(\mathbf{Y}^{\mathrm{p}_2}|\mathbf{Y}^{\mathrm{p}_1}) - h(\mathbf{Y}|\mathbf{X}) + h(\mathbf{Z}^{\mathrm{p}_1}|\mathbf{X}) \tag{25}$$

where $S^*_{p_{\mathbf{X}}}$ in (23) denotes the set of all input distributions having the optimal structure described in Lemma 5 and satisfying the power constraint in (1), matrix $\mathbf{Y}^{\mathrm{p}_2}$ in (24) is the collection of row vectors of $\mathbf{Y}$ with indices belonging to $\mathrm{p}_2 = \{1, \ldots, n_r\} \setminus \mathrm{p}_1$, and the inequality (25) follows from $h(\mathbf{Y}^{\mathrm{p}_1}) \leq h(\mathbf{Y}^{\mathrm{p}_1} + \mathbf{N}_e')$.

Now continuing from (25), we derive the desired upper bound in four steps.

In **step 1**, we derive an upper bound for $h(\mathbf{Y}^{\mathrm{p}_2}|\mathbf{Y}^{\mathrm{p}_1})$ in terms of $h(\mathbf{Y})$. We derive this upper bound by using the following general lemma.

Lemma 6 *Given an $m \times T$ random matrix $\mathbf{M}$ with entropy $h(\mathbf{M})$, for all $n \in \{1, \ldots, m\}$, there must exist a partition $(\mathrm{p}_1', \mathrm{p}_2')$ where $\mathrm{p}_1' \cup \mathrm{p}_2' = \{1, \ldots, m\}$, $|\mathrm{p}_1'| = n$, and $|\mathrm{p}_2'| = m - n$ such that*

$$h(\mathbf{M}^{\mathrm{p}_2'}|\mathbf{M}^{\mathrm{p}_1'}) \leq \frac{m-n}{m} h(\mathbf{M}) \tag{26}$$

where $\mathbf{M}^{\mathrm{p}_1'}$ and $\mathbf{M}^{\mathrm{p}_2'}$ denote the collection of row vectors of $\mathbf{M}$ with indices belonging to p_1' and p_2', respectively.

Now, from Lemma 6 and (25), we have

$$T \cdot C_s \leq \max_{p_{\mathbf{X}} \in S^*_{p_{\mathbf{X}}}} \frac{n_r - n_e}{n_r} h(\mathbf{Y}) - h(\mathbf{Y}|\mathbf{X}) + h(\mathbf{Z}^{\mathrm{p}_1}|\mathbf{X}) \tag{27}$$

which comes from the fact that for any partition $(\mathrm{p}_1, \mathrm{p}_2)$, (25) is a valid upper-bound.

In **step 2**, we derive an upper bound for $h(\mathbf{Y})$. Since given the input signal $\mathbf{X}$, each row vector of $\mathbf{Y}$ and $\mathbf{Z}^{\mathrm{p}_1}$ are i.i.d. Gaussian, the $-h(\mathbf{Y}|\mathbf{X}) + h(\mathbf{Z}^{\mathrm{p}_1}|\mathbf{X})$ term in (27) can be explicitly computed. In this step, we upper bound $h(\mathbf{Y})$ using the following lemma.

Lemma 7 *With the distribution of the channel input $\mathbf{X}$ satisfying the optimal structure in Lemma 5, the corresponding differential entropy of the legitimate receiver signal $\mathbf{Y}$ in* (11) *can be upper bounded as*

$$\max_{p_{\mathbf{X}} \in S^*_{p_{\mathbf{X}}}} h(\mathbf{Y}) \leq n_r^2 \log P + (T - n_r)\mathbb{E}\left[\log\det \mathbf{Y}\mathbf{Y}^\dagger\right] + o(\log P) \tag{28}$$

where $\lim_{P\to\infty} o(\log P)/\log P = 0$.

Now, from Lemma 7 and (27), we can further upper bound the secrecy capacity as

$$T \cdot C_s \leq \max_{p_{\mathbf{X}} \in S^*_{p_{\mathbf{X}}}} \frac{n_r - n_e}{n_r}(T - n_r)\mathbb{E}\left[\log\det \mathbf{Y}\mathbf{Y}^\dagger\right] - (n_r - n_e)\sum_{i=1}^{n_t} \mathbb{E}\left[\log(||\mathbf{X}_i||^2 + \sigma_r^2)\right] + n_e \sum_{i=1}^{n_t} \mathbb{E}\left[\log\left(\frac{||\mathbf{X}_i||^2 + \sigma_e^2}{||\mathbf{X}_i||^2 + \sigma_r^2}\right)\right] + (n_r - n_e) n_r \log P + o(\log P) \tag{29}$$

where $\mathbf{X}_i$ is the ith row of the given input signal $\mathbf{X}$.

By using the fact that $\log(1+x) \leq x$, we have

$$\mathbb{E}\left[\log\left(\frac{||\mathbf{X}_i||^2+\sigma_e^2}{||\mathbf{X}_i||^2+\sigma_r^2}\right)\right] \leq \mathbb{E}\left[\frac{\sigma_e^2-\sigma_r^2}{||\mathbf{X}_i||^2+\sigma_r^2}\right] \tag{30}$$

$$\leq \frac{\sigma_e^2-\sigma_r^2}{\sigma_r^2} \tag{31}$$

where the right hand side of (31) is a constant independent of P. From (29) and (31), we can upper bound the secrecy capacity $T \cdot C_s$ as

$$\begin{aligned}\max_{p_{\mathbf{X}} \in S^*_{p_{\mathbf{X}}}} (n_r-n_e)&\left(\frac{(T-2n_r)}{n_r}\mathbb{E}\left[\log\det \mathbf{Y}\mathbf{Y}^\dagger\right]\right.\\ &\left.+\mathbb{E}\left[\log\det \mathbf{Y}\mathbf{Y}^\dagger\right]-\sum_{i=1}^{n_t}\mathbb{E}\left[\log(||\mathbf{X}_i||^2+\sigma_r^2)\right]\right)\\ &+(n_r-n_e)n_r\log P+o(\log P)\end{aligned} \tag{32}$$

By the assumptions $T \geq 2n_r$ and $n_r > n_e$, we can obtain a further upper bound for (32) by developing upper bounds separately for $\mathbb{E}\left[\log\det \mathbf{Y}\mathbf{Y}^\dagger\right]$ and $\mathbb{E}\left[\log\det \mathbf{Y}\mathbf{Y}^\dagger\right] - \sum_{i=1}^{n_t}\mathbb{E}\left[\log(||\mathbf{X}_i||^2+\sigma_r^2)\right]$, respectively. In **step 3** and **step 4**, we will develop upper bounds for these two terms.

In **step 3**, we derive an upper bound for $\mathbb{E}\left[\log\det \mathbf{Y}\mathbf{Y}^\dagger\right]$ in (32) using the following lemma.

Lemma 8 *With the distribution of the channel input* $\mathbf{X}$ *satisfying the optimal structure in Lemma 5, and with* $n_t \geq n_r$*, the legitimate received signal* $\mathbf{Y}$ *in* (11) *satisfies*

$$\max_{p_{\mathbf{X}} \in S^*_{p_{\mathbf{X}}}} \mathbb{E}\left[\log\det \mathbf{Y}\mathbf{Y}^\dagger\right] \leq n_r\log P + o(\log P) \tag{33}$$

where $\lim_{P\to\infty} o(\log P)/\log P = 0$.

In **step 4**, we derive an upper bound for the combined term $\mathbb{E}\left[\log\det \mathbf{Y}\mathbf{Y}^\dagger\right] - \sum_{i=1}^{n_t}\mathbb{E}\left[\log(||\mathbf{X}_i||^2+\sigma_r^2)\right]$ in (32) using the following lemma.

Lemma 9 *With the distribution of the channel input* $\mathbf{X}$ *satisfying the optimal structure in Lemma 5, and with* $n_t \geq n_r$*, the legitimate received signal* $\mathbf{Y}$ *in* (11) *satisfies*

$$\max_{p_{\mathbf{X}} \in S^*_{p_{\mathbf{X}}}} \mathbb{E}\left[\log\det \mathbf{Y}\mathbf{Y}^\dagger\right] - \sum_{i=1}^{n_t}\mathbb{E}\left[\log(||\mathbf{X}_i||^2+\sigma_r^2)\right] \leq k \tag{34}$$

where k *is a constant which is independent of* P.

Finally, using Lemma 8 and Lemma 9 in (32), we obtain the desired upper bound on the s.d.o.f. as

$$D_s \leq (n_r-n_e)\left(\frac{T-n_r}{T}\right) \tag{35}$$

which completes the converse part of Lemma 2.

B. Achievable Scheme

In this part, we will show that a constant norm channel input [18], [19] transmitted on n_r antennas can achieve the s.d.o.f. upper bound given in (35). Specifically, let the channel input $\mathbf{X}_c$ be constant norm over n_r transmitted antennas and zero over the rest of $n_t - n_r$ antennas, i.e.,

$$\mathbf{X}_c = \text{diag}\left\{\sqrt{\frac{PT}{n_r}},\ldots,\sqrt{\frac{PT}{n_r}},0,\ldots,0\right\}\mathbf{\Theta} \tag{36}$$

where $\mathbf{\Theta}$ is an $T\times T$ i.d. unitary matrix. We can lower bound the achievable rate R_s as follows:

$$T\cdot R_s \geq I(\mathbf{X}_c;\mathbf{Y}) - I(\mathbf{X}_c;\mathbf{Z}) \tag{37}$$

$$= h(\mathbf{Y}) - h(\mathbf{Z}) - h(\mathbf{Y}|\mathbf{X}_c) + h(\mathbf{Z}|\mathbf{X}_c) \tag{38}$$

$$\begin{aligned}&= h(\mathbf{Y}) - h(\mathbf{Z})\\ &\quad - n_r\sum_{i=1}^{n_r}\log\left(\frac{PT}{n_r}+\sigma_r^2\right) - n_r(n_t-n_r)\log\sigma_r^2\\ &\quad + n_e\sum_{i=1}^{n_r}\log\left(\frac{PT}{n_r}+\sigma_e^2\right) + n_e(n_t-n_r)\log\sigma_e^2\end{aligned} \tag{39}$$

$$\geq h(\mathbf{Y}) - h(\mathbf{Z}) - (n_r-n_e)n_r\log P + o(\log P) \tag{40}$$

Since $\mathbb{E}[\text{tr}(\mathbf{Z}\mathbf{Z}^\dagger)] \leq (P+\sigma_e^2)n_eT$, the entropy $h(\mathbf{Z})$ of $\mathbf{Z}$ can be upper bounded by entropy of an i.i.d. Gaussian matrix as

$$h(\mathbf{Z}) \leq n_eT\log P + o(\log P) \tag{41}$$

As for the entropy of $\mathbf{Y}$, it can be shown that [19]

$$h(\mathbf{Y}) \geq h(\mathbf{H}\mathbf{X}_c) = n_rT\log P + o(\log P) \tag{42}$$

Thus, we have the following lower bound on the secrecy rate

$$T\cdot R_s = I(\mathbf{X}_c;\mathbf{Y}) - I(\mathbf{X}_c;\mathbf{Z}) \tag{43}$$

$$\geq (n_r-n_e)(T-n_r)\log P + o(\log P) \tag{44}$$

which implies

$$D_s \geq (n_r-n_e)\left(\frac{T-n_r}{T}\right) \tag{45}$$

This together with the upper bound in (35) gives the exact secure d.o.f. for the case $n_t \geq n_r > n_e$ and $T \geq 2n_r$ as

$$D_s = (n_r-n_e)\left(\frac{T-n_r}{T}\right) \tag{46}$$

completing the proof of Lemma 2.

As a final remark, we note that when $n_t \geq n_r$, we can use n_r transmitter antennas to achieve the optimal s.d.o.f. Having more than n_r transmit antennas gives us no improvement, at least, as far as the s.d.o.f. is concerned.

VI. Proof of Lemma 3

The proof is based on the key observation that when $n_t < n_r$, the receiver can use only n_t of its antennas without losing any s.d.o.f. That is, for a fixed n_t, the s.d.o.f. in the case where $n_t < n_r$ is, in fact, equal to the s.d.o.f. in the case with $n_r = n_t$. We state this formally in the following lemma.

Lemma 10 *For the MIMO legitimate channel* (2)*, if* $n_t < n_r$*, for any input signal* $\mathbf{X}$ *satisfying the power constraint in* (1)*, we have*

$$I(\mathbf{X};\mathbf{Y}) - I(\mathbf{X};\mathbf{Y}^{n_t}) \leq o(\log P) \tag{47}$$

where $\mathbf{Y}^{n_t}$ *denotes the collection of the first* n_t *row vectors of the received signal matrix* $\mathbf{Y}$*.*

Note that, in [19], a result similar to (47) but with more restrictions is proved as

$$\max_{p_{\mathbf{X}} \in S_{p_{\mathbf{X}}}} I(\mathbf{X};\mathbf{Y}) - \max_{p_{\mathbf{X}} \in S_{p_{\mathbf{X}}}} I(\mathbf{X};\mathbf{Y}^{n_t}) \leq o(\log P) \tag{48}$$

The inequality in (48) suffices to prove the results in [19] for block fading MIMO channels without secrecy constraints. However, it does not suffice in the case of block fading MIMO wiretap channel here. The reason is that we also need to consider the information leakage $I(\mathbf{X};\mathbf{Z})$ to the eavesdropper, and the $p_{\mathbf{X}}$ that maximizes $I(\mathbf{X};\mathbf{Y})$ may also be favorable for the eavesdropper. Thus, we need to derive a more general result than that in (48) in [19]; i.e., we need (47) which is valid for any input distribution $p_{\mathbf{X}}$ as given in Lemma 10.

To derive an upper bound for the s.d.o.f., we only focus on the case $\sigma_r^2 < \sigma_e^2$. When $n_r > n_e$ and $\sigma_r^2 < \sigma_e^2$, we can construct the same equivalent degraded channel in (18)-(19) and the secrecy capacity can be rewritten as in (20). The only difference here is that now the number of transmitter antennas is less than the number of legitimate receiver antennas, i.e., $n_t < n_r$. If we denote $\mathbf{X}^*$ as the optimal input for (20) when $n_t < n_r$, based on Lemma 10, we have

$$\begin{aligned} T \cdot C_s^{n_t<n_r} &= I(\mathbf{X}^*;\mathbf{Y}) - I(\mathbf{X}^*;\mathbf{Z}^{\mathrm{p}_1}) && (49)\\ &\leq I(\mathbf{X}^*;\mathbf{Y}^{n_t}) - I(\mathbf{X}^*;\mathbf{Z}^{\mathrm{p}_1}) + o(\log P) && (50)\\ &\leq \max_{p_{\mathbf{X}} \in S_{p_{\mathbf{X}}}} I(\mathbf{X};\mathbf{Y}^{n_t}) - I(\mathbf{X};\mathbf{Z}^{\mathrm{p}_1}) + o(\log P) && (51)\\ &= T \cdot C_s^{n_t=n_r} + o(\log P) && (52) \end{aligned}$$

where $C_s^{n_t<n_r}$ and $C_s^{n_t=n_r}$ are the secrecy capacity of the degraded equivalent channel (18)-(19) with $n_t < n_r$ and with $n_t = n_r$, respectively. We already know the s.d.o.f. when $n_r = n_t$ and $T \geq 2\min(n_t, n_r)$. For $n_r = n_t > n_e$, the s.d.o.f. D_s is given by (46) from Lemma 2, and for $n_r = n_t \leq n_e$, $D_s = 0$ from Lemma 1. Thus, when $n_t < n_r$ and $T \geq 2n_t$, we get the required upper bound as

$$D_s \leq (n_t - n_e)^+ \left(\frac{T - n_t}{T}\right) \tag{53}$$

The achievability of the above upper bound follows by using a constant norm channel input over n_t transmitter antennas as described previously. However, at the legitimate receiver, only n_t receiver antennas are needed and we can ignore the remaining $n_r - n_t$ row vectors of the received signal matrix $\mathbf{Y}$ while decoding at high SNR. These matching converse and achievability results complete the proof of Lemma 3.

VII. Conclusion

We considered the Rayleigh block fading wiretap channel with no a priori CSI at any of the terminals. We constructed a degraded equivalent channel, and determined its secrecy capacity. We determined the s.d.o.f. of this channel when $T \geq 2\min(n_t, n_r)$ to be $(\min(n_t, n_r) - n_e)^+(T - \min(n_t, n_r))/T$. When $\min(n_t, n_r) \leq n_e$, the s.d.o.f. is zero no matter how long the coherence time T is; an example of this is the scalar wiretap channel where $n_t = n_r = n_e = 1$. When $T = 1$, the s.d.o.f. is zero no matter how many antennas the transmitter and the legitimate receiver may have. We showed in this paper that when we have some moderate channel coherence together with multiple antennas at the legitimate entities, we can have non-zero s.d.o.f. The needed condition for this is that the legitimate entities have more antennas than the eavesdropper.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

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

[5] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[6] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 5515–5532, Nov. 2010.

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

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

[9] Y. Liang and H. V. Poor, "Secure communication over fading channels," in *Allerton Conference*, Sep. 2006.

[10] Z. Li, R. D. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Allerton Conference*, Sep. 2006.

[11] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[12] Z. Li, R. D. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Securing Wireless Communications at the Physical Layer*, R. Liu and W. Trappe, Eds. Springer US, 2010, pp. 1–18.

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

[14] Z. Li, R. D. Yates, and W. Trappe, "Achieving secret communication for fast rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 9, pp. 2792–2799, Sep. 2010.

[15] S.-C. Lin and C.-L. Lin, "On secrecy capacity of fast fading MIMOME wiretap channels with statistical CSIT," *IEEE Trans. Wireless Commun.*, submitted, Sep. 2013. Available at [arXiv:1309.1516].

[16] X. He and A. Yener, "MIMO wiretap channels with arbitrarily varying eavesdropper channel states," *IEEE Trans. Inf. Theory*, submitted, Jul. 2010. Available at [arXiv:1007.4801].

[17] P. Mukherjee and S. Ulukus, "Fading wiretap channel with no CSI anywhere," in *IEEE ISIT*, Jul. 2013.

[18] T. L. Marzetta and B. M. Hochwald, "Capacity of a mobile multiple-antenna communication link in Rayleigh flat fading," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 139 –157, Jan. 1999.

[19] L. Zheng and D. N. C. Tse, "Communication on the Grassmann manifold: A geometric approach to the noncoherent multiple-antenna channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 2, pp. 359–383, Feb. 2002.