Power Allocation and Achievable Secrecy Rates in MISOME Wiretap Channels

Thang Van Nguyen, *Student Member, IEEE*, and Hyundong Shin, *Senior Member, IEEE*

***Abstract*—We consider transmission of confidential data over multiple-input single-output multiple-eavesdropper (MISOME) Rayleigh-fading wiretap channels. The transmitter has access to *full* channel state information (CSI) of a legitimate link but only *partial* CSI of an eavesdropper link in forms of the average received signal-to-noise power ratio (SNR). In this location-aware scenario, we develop the optimal power allocation strategy that maximizes the secrecy rate achievable by beamforming. The optimal power control is regulated in an *on-off* fashion with the threshold depending only on the numbers of antennas and the average SNRs. By rescuing the vanishing high-SNR degree of freedom for secure communication from this optimal on-off beamforming with the *artificial noise* scheme, we further derive the achievable ergodic secrecy rate of MISOME wiretap channels in closed form.**

***Index Terms*—Achievable secrecy rate, artificial noise, MISOME, power allocation, Rayleigh fading, wiretap channel.**

I. Introduction

SHANNON laid the early foundations for information-theoretic security [1]—followed by Wyner [2]. Due to the inherent broadcast nature of the medium, wireless communication is susceptible to eavesdropping. Therefore, physical-layer security for wireless networks has recently received a great deal of interest and the treatment of Wyner's degraded discrete memoryless wiretap channel has been generalized and underpinned for characterizing the secrecy capacity of wireless channels (see, e.g., [3]–[6] and references therein).

In this letter, we consider transmission of confidential data over a multiple-input single-output Rayleigh-fading channel in the presence of a multiple-antenna eavesdropper—referred to as a multiple-input single-output multiple-eavesdropper (MISOME) wiretap channel [3]. In particular, the transmitter is assumed to have access to *full* channel state information (CSI) of a main legitimate channel but only *partial statistical* CSI of an eavesdropper channel. We show that the *on-off* power allocation is the optimal policy that maximizes the perfect secrecy rate achieved by beamforming in the direction of the legitimate channel. In [7], there is no power allocation across different fading states but only the power allocation among information-bearing signals and *artificial noise*. In contrast, we first treat the power allocation across different fading states without using artificial noise. We then derive the ergodic MISOME secrecy rate attained by this optimal on-off signaling in closed form. Due to a single degree of freedom for communication with (on-off) beamforming in the high signal-to-noise power ratio (SNR) regime for both the legitimate and eavesdropper channels, the degree of freedom for perfect secrecy transmission vanishes at high SNR. When the number of transmit antennas is larger than the eavesdropper antenna number, we can recover the high-SNR degree of freedom for secure communication by transmitting artificial noise in the null space of the legitimate channel [7].

Manuscript received July 12, 2011. The associate editor coordinating the review of this letter and approving it for publication was P. Popovski.

This work was supported by the Korea Research Foundation (NRF) grant funded by the Korea government(MEST) (No. 2011-0018071, 2011-0001274).

The authors are with the Department of Electronics and Radio Engineering, Kyung Hee University, Korea (e-mail: hshin@khu.ac.kr).

Digital Object Identifier 10.1109/LCOMM.2011.083011.111432

II. Problem Formulation

We consider a MISOME wiretap channel where an n_{t}-antenna transmitter sends confidential messages to a legitimate single-antenna receiver in the presence of an n_{e}-antenna eavesdropper. The received signals at the receiver and eavesdropper are given respectively by

$$y_{\mathrm{r}} = \sqrt{\mathsf{snr}_{\mathrm{r}}/n_{\mathrm{t}}}\,\boldsymbol{h}_{\mathrm{r}}\boldsymbol{x} + z_{\mathrm{r}} \tag{1}$$

$$\boldsymbol{y}_{\mathrm{e}} = \sqrt{\mathsf{snr}_{\mathrm{e}}/n_{\mathrm{t}}}\,\boldsymbol{H}_{\mathrm{e}}\boldsymbol{x} + \boldsymbol{z}_{\mathrm{e}} \tag{2}$$

where $\boldsymbol{x} \in \mathbb{C}^{n_{\mathrm{t}}}$ is the transmitted signal with the covariance matrix $\boldsymbol{\Sigma} \in \mathbb{C}^{n_{\mathrm{t}} \times n_{\mathrm{t}}}$ satisfying the power constraint $\mathrm{tr}\,(\boldsymbol{\Sigma}) \leq 1$; $\boldsymbol{h}_{\mathrm{r}} \sim \tilde{\mathcal{N}}_{1,n_{\mathrm{t}}}$ and $\boldsymbol{H}_{\mathrm{e}} \sim \tilde{\mathcal{N}}_{n_{\mathrm{e}},n_{\mathrm{t}}}$ are ergodic Rayleigh-fading channel gains from the transmitter to the receiver and eavesdropper, respectively; $z_{\mathrm{r}} \sim \tilde{\mathcal{N}}_{1,1}$ and $\boldsymbol{z}_{\mathrm{e}} \sim \tilde{\mathcal{N}}_{n_{\mathrm{e}},1}$ are additive white Gaussian noises; and $\mathsf{snr}_{\mathrm{r}}$ and $\mathsf{snr}_{\mathrm{e}}$ are the average received SNRs per antenna at the legitimate receiver and eavesdropper, respectively.[1] We use the convenient normalizations $\gamma_{\mathrm{r}} = \mathsf{snr}_{\mathrm{r}}/n_{\mathrm{t}}$ and $\gamma_{\mathrm{e}} = \mathsf{snr}_{\mathrm{e}}/n_{\mathrm{t}}$.

With perfect CSI at the receiver, the instantaneous perfect secrecy capacity in nat/s/Hz of MISOME wiretap channels is given by [3], [4]

$$C_{\mathrm{s}} = \max_{\substack{\boldsymbol{\Sigma}\succeq 0 \\ \mathrm{tr}(\boldsymbol{\Sigma})\leq 1}} \ln \left[\frac{1+\gamma_{\mathrm{r}}\boldsymbol{h}_{\mathrm{r}}\boldsymbol{\Sigma}\boldsymbol{h}_{\mathrm{r}}^{\dagger}}{\det\left(\mathbf{I}+\gamma_{\mathrm{e}}\boldsymbol{H}_{\mathrm{e}}\boldsymbol{\Sigma}\boldsymbol{H}_{\mathrm{e}}^{\dagger}\right)} \right] \tag{3}$$

where the superscript $(\cdot)^{\dagger}$ denotes conjugate transpose, $\mathbf{I}$ is the identity matrix, and $\mathbf{A} \succeq 0$ denotes that the matrix $\mathbf{A}$ is positive semidefinite. To optimize the input covariance $\boldsymbol{\Sigma}$ for secrecy capacity maximization in (3), the transmitter requires full CSI for both the legitimate and eavesdropper channels, which is infeasible in practice.[2] To practicalize this problem, we consider that the transmitter has full CSI only for the legitimate channel and partial CSI $\mathsf{snr}_{\mathrm{e}}$ for the eavesdropper

[1]The notation $\mathbb{C}$ denotes the complex field, $\mathrm{tr}\,(\cdot)$ is the trace operator, and $\boldsymbol{X} \sim \tilde{\mathcal{N}}_{m,n}$ denotes that $\boldsymbol{X}$ is the $m \times n$ complex Gaussian matrix whose entries are independent and identically distributed, circularly symmetric, zero-mean, unit-variance, complex Gaussian.

[2]The maximization in (3) is obtained by *beamforming* in the direction of the eigenvector corresponding to the largest eigenvalue of $\left(\mathbf{I}+\gamma_{\mathrm{e}}\boldsymbol{H}_{\mathrm{e}}^{\dagger}\boldsymbol{H}_{\mathrm{e}}\right)^{-1}\left(\mathbf{I}+\gamma_{\mathrm{r}}\boldsymbol{h}_{\mathrm{r}}^{\dagger}\boldsymbol{h}_{\mathrm{r}}\right)$ [3, Theorem 2].

channel with *location awareness*. For this amount of CSI at the transmitter, we can achieve the following secrecy rate for given $\boldsymbol{h}_{\mathrm{r}}$ using Gaussian codebooks:

$$R_{\mathrm{s}}^{(\mathrm{b})} = \max_{\substack{\boldsymbol{\Sigma}\succeq 0 \\ \mathrm{tr}(\boldsymbol{\Sigma})\leq 1}} \mathbb{E}_{\boldsymbol{H}_{\mathrm{e}}} \left\{ \ln \left[\frac{1+\gamma_{\mathrm{r}} \boldsymbol{h}_{\mathrm{r}} \boldsymbol{\Sigma} \boldsymbol{h}_{\mathrm{r}}^{\dagger}}{\det\left(\mathbf{I}+\gamma_{\mathrm{e}} \boldsymbol{H}_{\mathrm{e}} \boldsymbol{\Sigma} \boldsymbol{H}_{\mathrm{e}}^{\dagger}\right)} \right] \right\}. \quad (4)$$

Let $\lambda_1, \lambda_2, \ldots, \lambda_{n_{\mathrm{t}}}$ be the eigenvalues of $\boldsymbol{\Sigma}$ and $\lambda_{\max} = \max_i \lambda_i$. Then, it follows from the Rayleigh-Ritz theorem that

$$\begin{aligned} \ln\left(1+\gamma_{\mathrm{r}} \boldsymbol{h}_{\mathrm{r}} \boldsymbol{\Sigma} \boldsymbol{h}_{\mathrm{r}}^{\dagger}\right) &\leq \ln\left(1+\gamma_{\mathrm{r}} \lambda_{\max} \|\boldsymbol{h}_{\mathrm{r}}\|^2\right) \\ &\leq \ln\left(1+\gamma_{\mathrm{r}} \,\mathrm{tr}\left(\boldsymbol{\Sigma}\right) \|\boldsymbol{h}_{\mathrm{r}}\|^2\right). \end{aligned} \quad (5)$$

Let $\boldsymbol{\Lambda} = \mathrm{diag}\left(\lambda_1, \lambda_2, \ldots, \lambda_{n_{\mathrm{t}}}\right)$ and $\boldsymbol{h}_{\mathrm{e},i}$, $i = 1, 2, \ldots, n_{\mathrm{t}}$, denote the ith column of $\boldsymbol{H}_{\mathrm{e}}$. Then, we have

$$\begin{aligned} &\mathbb{E}_{\boldsymbol{H}_{\mathrm{e}}} \left\{ \ln\det\left(\mathbf{I}+\gamma_{\mathrm{e}} \boldsymbol{H}_{\mathrm{e}} \boldsymbol{\Sigma} \boldsymbol{H}_{\mathrm{e}}^{\dagger}\right) \right\} \\ &\quad \overset{(\mathrm{a})}{=} \mathbb{E}_{\boldsymbol{H}_{\mathrm{e}}} \left\{ \ln\det\left(\mathbf{I}+\gamma_{\mathrm{e}} \boldsymbol{H}_{\mathrm{e}} \boldsymbol{\Lambda} \boldsymbol{H}_{\mathrm{e}}^{\dagger}\right) \right\} \\ &\quad \overset{(\mathrm{b})}{\geq} \sum_{i=1}^{n_{\mathrm{t}}} \frac{\lambda_i}{\mathrm{tr}\left(\boldsymbol{\Sigma}\right)} \mathbb{E}_{\boldsymbol{h}_{\mathrm{e},i}} \left\{ \ln\det\left(\mathbf{I}+\gamma_{\mathrm{e}} \,\mathrm{tr}\left(\boldsymbol{\Sigma}\right) \boldsymbol{h}_{\mathrm{e},i} \boldsymbol{h}_{\mathrm{e},i}^{\dagger}\right) \right\} \\ &\quad \overset{(\mathrm{c})}{=} \sum_{i=1}^{n_{\mathrm{t}}} \frac{\lambda_i}{\mathrm{tr}\left(\boldsymbol{\Sigma}\right)} \mathbb{E}_{\boldsymbol{h}_{\mathrm{e},i}} \left\{ \ln\left(1+\gamma_{\mathrm{e}} \,\mathrm{tr}\left(\boldsymbol{\Sigma}\right) \|\boldsymbol{h}_{\mathrm{e},i}\|^2\right) \right\} \\ &\quad \overset{(\mathrm{d})}{=} \mathbb{E}_{W} \left\{ \ln\left(1+\gamma_{\mathrm{e}} \,\mathrm{tr}\left(\boldsymbol{\Sigma}\right) W\right) \right\} \end{aligned} \quad (6)$$

where $W \sim \mathsf{Erl}\left(n_{\mathrm{e}}, 1\right)$;[3] the equality (a) follows from the fact that the distribution of $\boldsymbol{H}_{\mathrm{e}}$ is unitary invariant; (b) follows from the fact that $\log\det\left(\cdot\right)$ is concave in positive semidefinite matrices and Jensen's inequality; (c) follows from the fact that $\det\left(\mathbf{I}+\mathbf{AB}\right) = \det\left(\mathbf{I}+\mathbf{BA}\right)$; and (d) follows from the fact that $\|\boldsymbol{h}_{\mathrm{e},i}\|^2 \sim \mathsf{Erl}\left(n_{\mathrm{e}}, 1\right)$ for all $i = 1, 2, \ldots, n_{\mathrm{t}}$. Note that the equality in (5) holds for beamforming in the direction of $\boldsymbol{h}_{\mathrm{r}}^{\dagger}$ (i.e., rank-one $\boldsymbol{\Sigma}$ with a nonzero eigenvector $\boldsymbol{h}_{\mathrm{r}}^{\dagger}/\|\boldsymbol{h}_{\mathrm{r}}\|$), whereas the equality in (6) is obtained by beamforming in any direction (i.e., any rank-one $\boldsymbol{\Sigma}$). Hence, the achievable rate $R_{\mathrm{s}}^{(\mathrm{b})}$ with perfect secrecy in (4) can be rewritten as

$$R_{\mathrm{s}}^{(\mathrm{b})} = \max_{0\leq\lambda\leq 1} \underbrace{\left[\ln\left(1+\lambda\gamma_{\mathrm{r}} \|\boldsymbol{h}_{\mathrm{r}}\|^2\right) - \mathbb{E}_{W}\left\{\ln\left(1+\lambda\gamma_{\mathrm{e}} W\right)\right\}\right]}_{R_{\mathrm{s}}(\lambda)}. \quad (7)$$

III. Power Allocation and Secrecy Rate

In this section, we develop the optimal power allocation that maximizes the achievable secrecy rate in (7) and derive the ergodic secrecy rate attained by this optimal power allocation.

A. Optimal Power Allocation

Theorem 1 (Optimal On-Off Signaling): Let

$$\lambda^{\star} = \arg\max_{0\leq\lambda\leq 1} R_{\mathrm{s}}\left(\lambda\right) \quad (8)$$

be the optimal value of λ that maximizes the secrecy rate $R_{\mathrm{s}}\left(\lambda\right)$ over $\lambda \in [0,1]$. Then, the optimal $\lambda^{\star}$ is the *on-off* power allocation

$$\lambda^{\star} = \begin{cases} 1, & \text{if } \|\boldsymbol{h}_{\mathrm{r}}\|^2 \geq \zeta \\ 0, & \text{otherwise} \end{cases} \quad (9)$$

with the threshold

$$\zeta = \frac{1}{\gamma_{\mathrm{r}}} \left[\exp\left\{ e^{1/\gamma_{\mathrm{e}}} \sum_{n=1}^{n_{\mathrm{e}}} E_n\left(\frac{1}{\gamma_{\mathrm{e}}}\right) \right\} - 1 \right] \quad (10)$$

where $E_n\left(z\right) = \int_1^{\infty} e^{-zt} t^{-n} dt$, $n = 0, 1, \ldots$, $\mathfrak{Re}\left\{z\right\} > 0$, is the nth-order exponential integral function [8].

Proof: Since

$$\frac{dR_{\mathrm{s}}\left(\lambda\right)}{d\lambda} = -\frac{1}{\lambda}\left[\frac{1}{1+\lambda\gamma_{\mathrm{r}}\|\boldsymbol{h}_{\mathrm{r}}\|^2} - \frac{e^{1/(\lambda\gamma_{\mathrm{e}})}}{\lambda\gamma_{\mathrm{e}}} E_{n_{\mathrm{e}}}\left(\frac{1}{\lambda\gamma_{\mathrm{e}}}\right) \right],$$

we have that $dR_{\mathrm{s}}\left(\lambda\right)/d\lambda \geq 0$ if and only if

$$\gamma_{\mathrm{r}} \|\boldsymbol{h}_{\mathrm{r}}\|^2 \geq \gamma_{\mathrm{e}} f\left(\frac{1}{\lambda\gamma_{\mathrm{e}}}\right) \quad (11)$$

where $f\left(t\right) \triangleq e^{-t}/E_{n_{\mathrm{e}}}\left(t\right) - t$, $t \geq 0$. Note that $df\left(t\right)/dt \geq 0$ if and only if

$$g\left(t\right) \triangleq \frac{2e^{-t}}{t+n_{\mathrm{e}}-1+\sqrt{\left(t+n_{\mathrm{e}}-1\right)^2+4t}} - E_{n_{\mathrm{e}}}\left(t\right) \geq 0 \quad (12)$$

and $dg\left(t\right)/dt \leq 0$ if and only if

$$1 - \frac{t+n_{\mathrm{e}}+1}{\sqrt{\left(t+n_{\mathrm{e}}-1\right)^2+4t}} \leq 0. \quad (13)$$

Since (13) holds for all $t \geq 0$ and $\lim_{t\to\infty} g\left(t\right) = 0$, the function $g\left(t\right)$ is nonnegative and monotonically decreasing (m.d.) and the inequality (12) holds for all $t \geq 0$. Hence, $f\left(t\right)$ is a monotonically increasing (m.i.) function for $t \geq 0$.

If there exists no solution for $dR_{\mathrm{s}}\left(\lambda\right)/d\lambda = 0$, then since $f\left(t\right)$ is m.i. for $t \geq 0$, $dR_{\mathrm{s}}\left(\lambda\right)/d\lambda > 0$ leading to $\lambda^{\star} = 1$. Suppose that λ_0 is the unique solution for $dR_{\mathrm{s}}\left(\lambda\right)/d\lambda = 0$. Then, since $g\left(t\right)$ is m.i. for $t \geq 0$, $R_{\mathrm{s}}\left(\lambda\right)$ is m.d. as a function of λ over $[0, \lambda_0]$, whereas $R_{\mathrm{s}}\left(\lambda\right)$ is m.i. for $\lambda \geq \lambda_0$. Therefore, the optimal value of λ that maximizes $R_{\mathrm{s}}\left(\lambda\right)$ over $\lambda \in [0,1]$ must be only $\lambda^{\star} = 1$ or $\lambda^{\star} = 0$. Furthermore, since $R_{\mathrm{s}}\left(0\right) = 0$ and $R_{\mathrm{s}}\left(\lambda\right)$ is increasing with $\|\boldsymbol{h}_{\mathrm{r}}\|^2$, we have $\lambda^{\star} = 1$ if and only if $\|\boldsymbol{h}_{\mathrm{r}}\|^2 \geq \zeta$, where ζ is the threshold value of $\|\boldsymbol{h}_{\mathrm{r}}\|^2$ for which $R_{\mathrm{s}}\left(1\right) = 0$, i.e.,

$$\gamma_{\mathrm{r}}\zeta = \exp\left[\mathbb{E}_{W}\left\{\ln\left(1+\gamma_{\mathrm{e}} W\right)\right\}\right] - 1, \quad (14)$$

from which along with the help of [8, eqs. (44) and (46)], we complete the proof. □

Remark 1: The optimal power allocation for beamforming to maximize the achievable secrecy rate is the on-off policy $\lambda^{\star} \sim \mathsf{Bern}\left(1-F_{\|\boldsymbol{h}_{\mathrm{r}}\|^2}\left(\zeta\right)\right)$ where $F_{\|\boldsymbol{h}_{\mathrm{r}}\|^2}\left(x\right)$ is the distribution of $\|\boldsymbol{h}_{\mathrm{r}}\|^2 \sim \mathsf{Erl}\left(n_{\mathrm{t}}, 1\right)$.[4] Note that Theorem 1 generalizes the on-off power control for a single-antenna wiretap channel in [5] to the MISOME channel.

Remark 2: The on-off threshold ζ decreases *inversely* with γ_{r}, whereas it grows with n_{e} and *asymptotically linearly* with γ_{e}. As $\gamma_{\mathrm{e}} \to \infty$, we have $\zeta \doteq \gamma_{\mathrm{e}}$, which follows from the fact that $e^{1/z} \doteq 1$, $E_1\left(1/z\right) \doteq \ln\left(z\right)$, and $E_k\left(1/z\right) \doteq 1$ for $k \geq 2$ as $z \to \infty$.[5] In particular, we get from (10) that

$$\zeta_{\inf(\alpha)} \triangleq \lim_{\substack{\gamma_{\mathrm{r}},\gamma_{\mathrm{e}}\to\infty \\ \gamma_{\mathrm{r}}/\gamma_{\mathrm{e}}\to\alpha}} \zeta = \alpha \exp\left(-\gamma + \sum_{n=1}^{n_{\mathrm{e}}-1} \frac{1}{n}\right) \quad (15)$$

[3] $\mathsf{Erl}\left(n, \lambda\right)$ denotes the nth-order Erlang distribution with a hazard rate λ.

[4] $\mathsf{Bern}\left(p\right)$ denotes the Bernoulli distribution with mean p.

[5] The symbol $\doteq$ denotes asymptotically exponential equality.

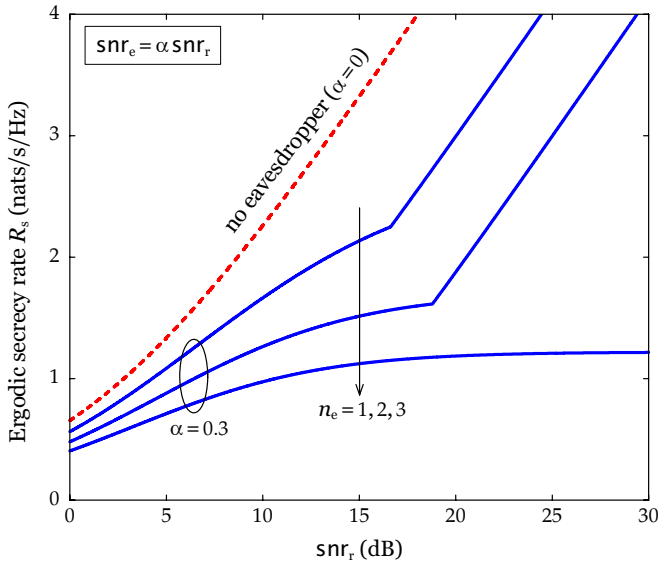

Fig. 1. Ergodic secrecy rate $R_{\rm s}$ versus $\mathsf{snr}_{\rm r}$ when $n_{\rm t}=3$ and $\mathsf{snr}_{\rm e}=\alpha\,\mathsf{snr}_{\rm r}$.

where $\gamma\approx 0.5772156649$ is the Euler-Mascheroni constant. This asymptotic on-off threshold $\zeta_{\inf(\alpha)}$ increases with α and $n_{\rm e}$, while not depending on $n_{\rm t}$.

B. Ergodic Secrecy Rate

Theorem 2: The ergodic secrecy rate (nats/s/Hz) of MISOME Rayleigh-fading wiretap channels achieved by beamforming with the on-off power allocation $\lambda^\star$ is given by

$$\langle R_{\rm s}^{(\rm b)}\rangle_\zeta = e^{1/\gamma_{\rm r}}\sum_{n=1}^{n_{\rm t}}\sum_{k=1}^{n}\frac{\zeta^{n_{\rm t}-n}}{(n_{\rm t}-n)!}E_k\left(\zeta+\frac{1}{\gamma_{\rm r}}\right). \qquad (16)$$

Proof: It follows from (7), (14), and Theorem 1 that

$$\begin{aligned}\langle R_{\rm s}^{(\rm b)}\rangle_\zeta &= \mathbb{E}\left\{R_{\rm s}(1)\,\middle|\,\|\boldsymbol{h}_{\rm r}\|^2\geq\zeta\right\}\mathbb{P}\left\{\|\boldsymbol{h}_{\rm r}\|^2\geq\zeta\right\}\\ &= \int_\zeta^\infty \ln\left(\frac{1+\gamma_{\rm r}x}{1+\gamma_{\rm r}\zeta}\right)dF_{\|\boldsymbol{h}_{\rm r}\|^2}(x)\\ &= e^{-\zeta}\sum_{n=1}^{n_{\rm t}}\left[\binom{n_{\rm t}-1}{n-1}\frac{\zeta^{n_{\rm t}-n}}{(n_{\rm t}-1)!}\right.\\ &\quad\left.\times\int_0^\infty \ln\left(1+\frac{\gamma_{\rm r}x}{1+\gamma_{\rm r}\zeta}\right)x^{n-1}e^{-x}dx\right]. \qquad (17)\end{aligned}$$

By evaluating the integral in (17) again with the help of [8, eqs. (44) and (46)], we arrive at the desired result (16). □

Remark 3: It is also easy to show that $d\langle R_{\rm s}^{(\rm b)}\rangle_\zeta/d\zeta\leq 0$ for fixed $\gamma_{\rm r}$. Hence, $\langle R_{\rm s}^{(\rm b)}\rangle_\zeta$ decreases with ζ (or equivalently with $n_{\rm e}$ and $\gamma_{\rm e}$). In particular, at $\gamma_{\rm e}=0$ (no eavesdropper), we have $\zeta=0$ and hence, (16) reduces exactly to [8, eq. (20)] for the ergodic capacity without secrecy constraints.

Remark 4: The ergodic secrecy rate converges to a limiting constant $\langle R_{\rm s}^{(\rm b)}\rangle_{\inf(\alpha)}$ in the asymptotic regime, where $\gamma_{\rm r}$ and $\gamma_{\rm e}$ tend to infinity with $\gamma_{\rm e}/\gamma_{\rm r}\to\alpha$. This reveals that the degree of freedom for perfect secrecy transmission vanishes due to a single high-SNR degree of freedom for communication by transmit beamforming in both the legitimate and eavesdropper channels. However, we can rescue this high-SNR behavior of the ergodic secrecy rate by exploiting artificial noise when $n_{\rm e}<n_{\rm t}$ [7]. By transmitting the information-bearing signal and the artificial noise in the direction and null space of the legitimate channel, respectively, the artificial noise behaves as interference only in the eavesdropper channel and hence removes the high-SNR communication degree for eavesdropping with no effect on the legitimate link. Using the secrecy rate $\langle R_{\rm s}^{(\rm a)}\rangle$ attained by the artificial noise scheme [7, eq. (13)] at high SNR, we get the achievable ergodic secrecy rate as[6]

$$R_{\rm s}=\max\left\{\langle R_{\rm s}^{(\rm b)}\rangle_\zeta,\langle R_{\rm s}^{(\rm a)}\rangle\right\}. \qquad (18)$$

Example 1: Fig. 1 shows the achievable ergodic secrecy rate $R_{\rm s}$ as a function of $\mathsf{snr}_{\rm r}$ when $n_{\rm t}=3$ and $\mathsf{snr}_{\rm e}=\alpha\,\mathsf{snr}_{\rm r}$ for $\alpha=0$ (no eavesdropper), 0.3 and $n_{\rm e}=1$, 2, 3. We observe that the on-off beamforming recovers a positive ergodic secrecy rate in the low-SNR regime, whilst the artificial noise rescues the degree of freedom for secure communication at high SNR for $n_{\rm e}<n_{\rm t}$. Let $\mathsf{snr}_{\rm r}^\star$ be the value of $\mathsf{snr}_{\rm r}$ at which $\langle R_{\rm s}^{(\rm b)}\rangle_\zeta=\langle R_{\rm s}^{(\rm a)}\rangle$ (for example, 16.62 dB and 18.79 dB for $n_{\rm e}=1$ and 2 in Fig. 1). Then, the ergodic secrecy rate $R_{\rm s}$ is achieved by i) beamforming with on-off power allocation in the SNR regime $\mathsf{snr}_{\rm r}\leq\mathsf{snr}_{\rm r}^\star$; and ii) adaptive-power beamforming for information and artificial nosing in the regime $\mathsf{snr}_{\rm r}>\mathsf{snr}_{\rm r}^\star$.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.
[3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.
[4] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE International Symposium on Information Theory*, July 2008.
[5] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[6] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, June 2009.
[7] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
[8] H. Shin and J. H. Lee, "Capacity of multiple-antenna fading channels: spatial fading correlation, double scattering, and keyhole," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2636–2647, Oct. 2003.

[6]Note that [7, eq. (13)] is obtained by considering the worst-case scenario such that the noise at the eavesdropper is arbitrarily small.